(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 July 2001 (12.07.2001)

PCT

(10) International Publication Number
WO 01/50224 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US00/32798

(22) International Filing Date: 4 December 2000 (04.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/174,436 4 January 2000 (04.01.2000) US
60/206,842 24 May 2000 (24.05.2000) US

(71) Applicant *(for all designated States except US)*: CHIPPO TECHNOLOGIES, INC. [—/—]; Ugland House, P.O. Box 309, George Town (KY).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: LIN, Robin [US/—]; 9F, #1 Lane 124 Sec 1, Chien Kuo North Road, Taipei (TW). CHRISTIAANSEN, Geert [NL/NL]; Sleedoorn 27, NL-5708 DE Helmond (NL).

(74) Agents: PIRIO, Maurice, J. et al.; Perkins Coie LLP, P.O. Box 1247, Seattle, WA 98111-1247 (US).

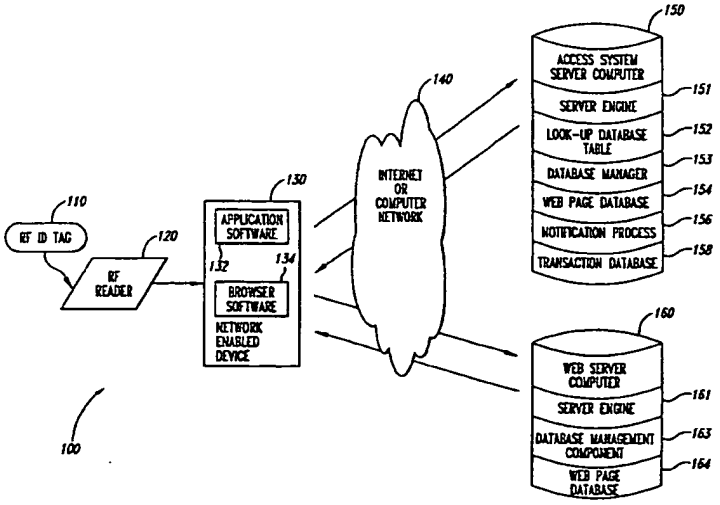
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHODS AND SYSTEMS FOR ACCESSING INFORMATION AND SERVICES ON A COMPUTER NETWORK



(57) Abstract: A facility for automatically accessing information and/or services on a computer network is described. The facility transmits a request for information and/or services by reading a unique code off of a computer-readable medium, and transmitting the unique code to a server computer using a network-enabled device. In response to receiving the unique code, the server computer retrieves selected data from a database table, the selected data being linked to the unique code in the database table. The selected data is then provided to the network-enabled device. In one embodiment, the selected data can include a web site or an application program. In another embodiment, the selected data can include a URL. When a URL is provided to the network-enabled device, the facility can launch a browser program on the network-enabled device to retrieve the information and/or services associated with the URL.

WO 01/50224 A2

METHODS AND SYSTEMS FOR ACCESSING INFORMATION AND SERVICES ON A COMPUTER NETWORK

TECHNICAL FIELD

The present invention is directed to the field of electronic commerce and, more particularly, to methods and systems for marketing products and services using a computer network.

BACKGROUND

Because it facilitates electronic communications between vendors and purchasers, the Internet is increasingly being used to conduct "electronic commerce." The Internet comprises a vast number of computers and computer networks that are interconnected through communication channels. Electronic commerce refers generally to commercial transactions that are at least partially conducted using the computer systems of the parties to the transactions. For example, a purchaser can use a personal computer to connect via the Internet to a vendor's computer. The purchaser can then interact with the vendor's computer to conduct the transaction. Although many of the commercial transactions that are performed today could be performed via electronic commerce, the acceptance and widespread use of electronic commerce depends, in large part, upon the ease-of-use of conducting such electronic commerce. If electronic commerce can be easily conducted, then even the novice computer user will choose to engage in electronic commerce. Therefore, it is important that techniques be developed to facilitate conducting electronic commerce.

The Internet facilitates conducting electronic commerce, in part, because it uses standardized techniques for exchanging information. Many standards have been established for exchanging information over the Internet, such as electronic mail, Gopher, and the World Wide Web ("WWW"). The WWW service allows a server computer system (*i.e.*, web server or web site) to send graphical web pages of information to a remote client computer system. The remote

client computer system can then display the web pages. Each resource (*e.g.*, computer or web page) of the WWW is uniquely identifiable by a Uniform Resource Locator ("URL"). To view a specific web page, a client computer system specifies the URL for that web page in a request (*e.g.*, a HyperText Transfer Protocol ("HTTP") request). The request is forwarded to the web server that supports that web page. When that web server receives the request, it sends the requested web page to the client computer system. When the client computer system receives that web page, it typically displays the web page using a browser. A browser is typically a special-purpose application program that effects the requesting of web pages and the displaying of web pages.

The World Wide Web portion of the Internet is especially conducive to conducting electronic commerce. Many web servers have been developed through which vendors can advertise and sell products. The products can include items (*e.g.*, music) that are delivered electronically to the purchaser over the Internet and items (*e.g.*, books) that are delivered through conventional distribution channels (*e.g.*, a common carrier). A server computer system may provide an electronic version of a catalog that lists the items that are available. A user, who is a potential purchaser, may browse through the catalog using a browser and select various items that are to be purchased. When the user has completed selecting the items to be purchased, the server computer system then prompts the user for information to complete the ordering of the items. This purchaser-specific order information may include the purchaser's name, the purchaser's payment information (*e.g.*, credit card number), and a shipping address for the order. The server computer system then typically confirms the order by sending a confirming web page to the client computer system and schedules shipment of the items.

Along with the explosive growth of the Internet and the World Wide Web, users are finding it more and more difficult to easily locate desired information and conduct electronic commercial transactions. Complicated URL addresses, layers of topic sub-menus, and search engines that produce thousands of web sites per search, are making use of the Internet less friendly and more time consuming. Similarly, some aspects of electronic commerce (*e.g.*, cyber cash and online shopping), where transactions happen "automatically" in cyberspace and thus beyond the user's consent or control, leave the user with a sense of loss of control.

In order to view and navigate web sites on the Internet using an Internet-enabled device such as a personal computer, a user typically must use a modem to dial in to an ISP (Internet service provider), and then start up an Internet browser program. To reach a desired web site, the user may type in a specific URL address in the "address" box of the browser program, or use a search engine and click on the selection found to be most appropriate. When typing in a new URL address, the user will have made the effort to either write down or memorize the URL address, and then correctly type the address into the "address" box without syntax or spelling errors. Both activities are troublesome, time consuming, and prone to human error. Failure to accomplish both correctly, however, will lead to a failed search or arrival at an undesired web site.

Similarly, when using a search engine to reach a desired web site, the user types in a word or words of an item or topic for which the user wishes to search. The search engine will use the word or words specified, regardless of context, to generate a result from the engine's scans of the entire Internet. As there are million of web sites around the world, this search often results in thousands of options for a given search. The user is thus overloaded with seemingly appropriate options and often is unable to discover the actual web site that the user was truly searching for.

The shortcomings associated with searching for information or services on the Internet using the customary methods of typing in URL addresses or scanning search engine results often discourages users to the point of aborting their search. Thus, it would be desirable to have a system that simplifies access to information or services on the Internet by allowing the user to automatically and quickly go to precisely the web site desired.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a schematic diagram illustrating components of an access system in one embodiment.

Figure 2 is a flow diagram of a routine performed by application software for retrieving information and/or services from a server computer using the access system in one embodiment.

Figure 3 is a flow diagram of a routine performed on a server computer for responding to a unique transaction code ("UTC") request in one embodiment.

Figure 4 is a flow diagram of a routine performed by application software for selecting between launching a local application or retrieving a URL from a remote server computer, in another embodiment.

Figure 5 is a schematic diagram illustrating the assembly of a unique 10-byte RF reader code in one embodiment.

Figure 6 is a schematic diagram illustrating the assembly of a UTC in one embodiment.

Figure 7 is a flow diagram of a routine performed on a server computer for communicating with a network-enabled device in a secure mode in one embodiment.

Figure 8 is a flow diagram of a routine performed on a user network-enabled device for communicating with a server computer in a secure mode in one embodiment.

Figure 9 is a flow diagram of a routine performed by application software for retrieving information and/or services from a server computer using the access system in one embodiment.

Figure 10 is a schematic diagram illustrating the assembly of an RF reader code in an alternative embodiment.

Figure 11 is a schematic diagram illustrating the assembly of a registration RF tag code in an alternative embodiment.

Figure 12 is a schematic diagram illustrating the assembly of a new user command code in an alternate embodiment.

Figure 13 is a schematic diagram illustrating the assembly of a UTC in an alternate embodiment.

Figure 14 is a schematic diagram illustrating the assembly of a unique 64-bit RF tag code in one embodiment.

Figure 15 is a schematic diagram illustrating the assembly of a unique 256-bit RF tag code in one embodiment.

DETAILED DESCRIPTION OF THE ILLUSTRATED EMBODIMENTS

Methods and systems for simplifying a user's access to resources on the Internet are provided. The access system allows a user to view a web page, download content (including streaming audio and video content), conduct a commercial transaction, or perform virtually any other Internet related activity by placing a computer-readable medium, such as a radio-frequency identification tag ("RF tag"), in the proximity of a computer-readable medium reader, such as a radio-frequency read/write device ("RF reader"), that communicates with the user's network-enabled device such as a computer. The user can obtain the desired information and/or service without having to search for the appropriate web site and without having to key the exact URL into the address box of a browser program. One skilled in the art would appreciate that the computer-readable medium may include a magnetic medium, any laser-readable medium, and so on.

In one embodiment, an RF tag and RF reader are each encoded with unique codes that are also stored in a system server computer and entered into a look-up database table that links each unique code with a specific application, server, or web site URL. The RF tag can be embedded in a token, financial instrument, consumer product, promotional item, and so on for distributing to a consumer/user via a purchased product, advertising, or promotional activity. Similarly, an RF reader can be given to users as a promotional item or it can be purchased by the user. Application software loaded on a network-enabled device of the user interfaces with the RF reader. Like the RF tag and RF reader, this application software can be purchased by the user or distributed (*e.g.*, via the Internet) to the user for free as a promotional item.

When the user wants to access resources such as information or services on a desired web site using the access system, the user places an appropriate RF tag in the proximity of the RF reader. The RF reader reads the unique code off of the RF tag, and sends the RF tag's unique code and, in one embodiment, the RF reader's code to the user's network-enabled device via a wired or wireless connection. The application software running on the user's network-enabled device receives the two unique codes and combines them into a single unique transaction code (UTC). The application software then establishes access to the Internet or other suitable computer network, and sends the UTC via the network

to the system server computer having the look-up database tables that map the code (*i.e.*, the unique codes from the RF tag and the RF reader) to a specific application, server, or web site URL.

The system server computer then extracts the RF tag's unique code from the UTC and matches it against the codes in the look-up database tables. When the RF tag's unique code is found, the system server computer sends, in one embodiment, the URL associated with that unique code to the application software on the user's network –enabled device. The application software receives this URL and directs a browser program on the network-enabled device to retrieve the information (*e.g.*, web page) or application associated with the URL. Once retrieved, the user is able to use the information or run the application to view the information, perform a desired commercial transaction, or any other activity.

The access system can be used in various embodiments to provide the user with easy access to information or services. For example, the RF tag can be encoded with a unique code that, rather than access a URL via a remote server computer, simply initiates a local application on the user's network-enabled device. Alternatively, a "simple RF tag" can be encoded with a unique code that contains a specific URL. In this embodiment, the simple RF tag is placed in the proximity of the RF reader, and the reader reads the URL off of the RF tag and transmits this URL to the application software on the user's network-enabled device. The application software then launches a browser program with the URL and retrieves the associated content or application for the user to view, download, or otherwise interact with. In the "simple RF tag" embodiment, there is no need for the application software to first access the system server computer to retrieve the URL, as the URL is encoded directly into the RF tag.

RF tags can also be encoded with unique codes that cause the system server computer to perform transactions in a secure mode. In secure embodiments, the RF tag's unique code is linked to a security routine of the system server computer. The security routine directs the system server computer to request that the application software send it a password encoded on the RF tag. In one embodiment, this can be a 32-bit password, in other embodiments, the password can contain more or less than 32 bits of information. After the system server computer receives the password from the application software and checks it for authenticity,

the transaction is allowed to proceed and, in one embodiment, the system server computer sends a new password back to the application software. The application software can then direct the RF reader to write (assuming write capability) this new password onto the RF tag. The new password can then be used in subsequent secured transactions.

In an alternate embodiment, a remote web server computer that receives a URL request from the application software can perform a secure password exchange routine that is substantially similar to the routine discussed above with reference to the system server computer. In this embodiment, the web server computer would request the application software send it the 32-bit password encoded on the RF tag for verification of authenticity. After verification, the web server computer could send a new password back to the application software. The application software can then direct the RF reader to write (assuming write capability) this new password onto the RF tag. The new password can then be used in subsequent secured transactions. All password exchange communications between the application software and server computers can be in secure mode (*e.g.*, SSL, PCT, or TLS).

Although not required, embodiments of the access system will be described in the general context of computer executable instructions, such as routines executed by a general-purpose computer, such as a personal computer. Those skilled in the art will appreciate that the access system can be practiced with other computer system configurations, including Internet appliances, hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, mini-computers, mainframe computers, and the like. The access system can be embodied in a special-purpose computer or data processor that is specifically programmed, configured or constructed to perform one or more of the computer-executable instructions explained in detail below. The access system can also be implemented in distributed computing environments where tasks or modules are performed by remote processing devices, which are linked through a wired or wireless communications network. In a distributed computing environment, program modules or subroutines may be located in both local and remote memory storage devices.

Figure 1 is a schematic diagram illustrating components of an access system in one embodiment. An access system 100 includes a uniquely coded radio-frequency identification tag 110 ("RF tag 110"), and a uniquely coded radio-frequency read/write device 120 ("RF reader 120"). The RF reader 120 is capable of reading the unique radio-frequency code off of the RF tag 110, and writing information to the RF tag 110. In one aspect of this embodiment, the RF reader can be masked to only read RF codes off selected RF tags, in this way preventing the use of unauthorized or copied RF tags. The RF reader 120 transmits the RF tag's unique code, and its own unique code, to a user network-enabled device 130 ("user computer 130"). In one embodiment, the unique codes are transmitted to the user computer 130 via a wired connection. In one aspect of this embodiment, the RF reader connects to the user computer via a Universal Serial Bus (USB), and connects to the USB host as a Human Input Device (HID Class). Alternatively, the wired connection can be IEEE 1394, DVI, or PS/2. In another embodiment, the unique codes are transmitted via a wireless connection. In one aspect of this embodiment, the wireless connection can be infrared (*e.g.*, IrDA), or radio frequency (*e.g.*, Bluetooth or HomeRF).

In other embodiments, the RF tag can be replaced by a suitable tag that uses a magnetic strip (such as a credit card), a bar code, or other method of encoding a computer readable medium. Accordingly, the RF reader can be replaced by a device suitable for reading and writing to the corresponding tag embodiment.

The user computer 130 may include one or more central processing units or other logic processing circuitry, memory, input devices (*e.g.*, keyboards and pointing devices), output devices (*e.g.*, display devices and printers), and storage devices (*e.g.*, fixed, floppy and optical disk drives), all well known but not shown in Figure 1. The user computer 130 may include a browser program module 134 ("browser 134") that allows the user computer 130 to access and exchange data with a computer network 140, including web sites within the World Wide Web portion of the Internet. The user computer 130 also includes an application software module 132 that performs the functions of reading the unique RF codes of the RF tag 110 and RF reader 120, writing information to the RF tag 110, and other routines associated with accessing information and services off of the computer network 140, as described in further detail below.

As best seen in Figure 1, the user computer 130 is connected via the computer network 140 to a system server computer 150 and a web server computer 160. The system server computer 150 performs many of the processes associated with the access system 100, and includes a look-up database table 152 that stores the unique codes from the RF tag 110 and RF reader 120. The look-up database table 152 maps each specific unique code to a specific application, server computer, or web site URL that is accessed via the computer network 140. One skilled in the art will appreciate that mapping techniques other than a look-up table can be used. The system server computer 150 also includes a server engine 151, a database management component 153, a web page database 154, a notification process component 156, and a transaction database 158, as well as other components not shown in Figure 1.

The web server computer 160 includes a server engine 161, a database management component 163, and a web page database 164, as well as other components not shown in Figure 1. The web server computer 160 can store content and applications and distribute them via the computer network 140 to the user computer 130. The content can be in audio, video, or graphical format and the applications can perform commercial transactions or data management functions.

One skilled in the art will appreciate that concepts of the access system can be used in various environments other than the Internet or computer network environment depicted in Figure 1. For example, the concepts can also be used in electronic mail environments in which the electronic mail messages may include the equivalent of a unique RF code, or an associated web page or URL. In one aspect of this embodiment, the information the user retrieves can be presented to the user as an email message, or as an email message with a hyperlink to a web site. Various communication channels other than the Internet may also be used, such as a local area network, a wide area network, or a point-to-point dial-up connection. Concepts of the access system may also be used in a single computer environment rather than a user/server environment. In addition, the system server computer 150 may comprise any combination of hardware or software that can support these concepts. In particular, the access system server computer 150 may actually include multiple computers. Similarly, the user network-enabled device 130 may comprise any combination of hardware or software that interacts with the

system server computer 150 to perform the concepts of the access system disclosed herein. This user device may include television-based systems, and various other consumer products through which web pages may be accessed. For example, computer-readable medium may be a device that sends its unique code as a telephonic tone when activated. The code may identify a web page and be used by a web-enabled phone to retrieve and display the web page.

Figure 2 is a flow diagram of a routine 200 performed by the application software 132 for retrieving information and/or services from a server computer using the access system 100 in one embodiment. In block 202, the routine 200 checks for the presence of the RF tag 110 in the proximity of the RF reader 120. In decision block 204, if the RF tag 110 is not presently in the proximity of the RF reader 120, the routine 200 continues to check for the presence of an RF tag. If the RF tag 110 is in the proximity, then the routine 200 obtains the RF tag's unique code from the RF reader 120, as shown in block 206. One skilled in the art would appreciate that this routine could be invoked when, or wait for, an event to be generated indicated that the RF tag is in proximity of RF reader. In block 208, the routine 200 obtains the RF reader's unique code from the RF reader 120 as well. In block 210, the routine 200 combines the unique codes from the RF tag 110 and the RF reader 120 and creates a unique transaction code (UTC). In block 212, the routine 200 establishes a connection to the computer network 140 and sends the UTC via the computer network 140 to the system server computer 150. The routine 200 then receives a corresponding URL back from the system server computer 150 via the computer network 140, as shown in block 214. In block 216, the routine 200 launches the browser 134 with the URL received from the system server computer 150. In an alternate embodiment of block 216, the routine 200 can launch a local application program received from the system server computer 150 instead of the URL received in block 214. After performing block 216, the routine 200 loops to block 202 to wait for an RF tag.

In a separate routine not shown but well known in the relevant art, the browser 134 in block 216 sends the URL via the computer network 140 to the web server computer 160. The web server computer 160 responds by sending the appropriate web page back to the browser 134, which the browser 134 will then display on the user computer 130. In other aspects of this embodiment, the web

server computer 160 can send audio or video content, or web pages formatted for commercial transactions or data management, to the browser 134.

In addition to performing the routine 200, the application software 132 can also include a routine or routines that allow a user to use the access system without having to place an actual RF tag in the proximity of the RF reader. For example, when an RF tag is first used, the server computer can provide a bitmap or code to the application software 132 for creating a graphic image of the RF tag on the user's network-enabled device. The application software 132 can then use the code in a directory routine that compiles, sorts, and displays a user's RF tags on the user's network-enabled device based on information contained in the RF tag's unique RF identification code. The RF tags can be sorted into different fields by different criteria, such as the shape of the RF tag, application type, date the RF tag was first used, color of the RF tag, etc. Once an RF tag's data has been stored in the directory, the RF tag can be graphically presented as a "virtual" RF tag and displayed on the user's network-enabled device. The user can then start a transaction as if the "real" RF tag was being used simply by "clicking on" the virtual RF tag in the directory.

In a similar way, the server computer can also provide the application software 132 with an audio code for presenting an audible display whenever a particular RF tag is used. For example, a theme song or advertising jingle associated with a particular product can be audibly displayed when an RF tag associated with that product is used.

The application software 132 can also include its own browser routine that can serve as the network navigation program, with pre-installed applications that can speed up, facilitate, and/or simplify usage of the access system when linked to the computer network 140. In addition to retrieving the desired content from a selected web site URL, the application software can also display a greeting card that calls up humorous video clips, digital photo albums, birthday songs, etc. as an added dimension of the interactivity offered by the access system. The application software 132 can also include other facilities, such as look-up tables that map the unique identification codes of the RF tag 110 and RF reader 120 to specific applications, servers, or web site URLs. Compilation of user-specific information

and data, such as web sites visited, transactions performed, and times used, can also be accomplished with the application software 132.

Figure 3 is a flow diagram of a routine 300 performed by server software for responding to a UTC request in one embodiment. In block 302, the routine 300 receives a UTC from a resource such as the application software 132. In decision block 304, the routine 300 checks the UTC to determine if the UTC is valid. If not, the routine 300 sends an error message to the user computer 130, as shown in block 310. If the UTC is valid, the routine 300 extracts the RF tag's unique code from the UTC as shown in block 305. In block 306, the routine 300 retrieves the URL corresponding to this code from the look-up database table 152 of the system server computer 150. The routine 300 then sends this URL to the resource that sent the UTC, such as the application software 132. The transaction in block 307 can be stored in the transaction database 158 of the system server computer 150, as shown in block 308. After performing block 308, the routine 300 loops to block 302 to receive a UTC.

In one aspect of this embodiment not shown in Figure 3, the routine 300 can extract the unique code for the RF reader 120 from the UTC sent to it by the application software 132. The routine 300 can then determine if the RF reader 120 is the most up-to-date version. If not, the routine 300 can send an appropriate message to the application software 132 for display to the user that indicates that an update to the RF reader 120 is advisable. In a similar process, the routine 300 can also check the version of application software 132 running on the user computer 130, and include a message recommending an update if the application software 132 is not found to be the most up-to-date version.

In addition to the routine 300 discussed above, the system server computer 150 can also perform other functions. For example, it can keep track of all RF tags used by a particular user, and/or record other personal user data. The server computer 150 can then organize this user data and perform data mining and data analysis operations with the compiled information. This information can then be accessed by commercial clients for marketing purposes when the client uses a dedicated authorization RF tag. As will be discussed below, the system server computer 150 is also able to initiate and terminate secure communications with the application software 132 and/or the web server computer 160. Included in the

secure functions is the ability to verify the authenticity of the RF tag 110 via a password encoded on the RF tag, and the ability to provide a new password to be written to the RF tag 110 over the original password. In addition, the server computer 150 can also act as a host server for specific application web sites that are accessed by "simple" unlinked RF tags that are encoded with URLs.

Figure 4 is a flow diagram of a routine 400 performed by the application software 132 for selecting between launching a local application or retrieving a URL from a remote server computer, in another embodiment. In one aspect of this embodiment, there are three types of RF tags available: a 64-bit type 1 RF tag, a 256-bit type 2 RF tag, and a 2,048-bit type 3 RF tag. The type 1 RF tag is a read-only device without a password that can be used with the computer network 140 for non-secure applications like retrieving advertising, samplers of audio/video, or greeting cards. The type 2 RF tag can be read and written to, and contains a 32-bit password. The type 2 RF tag can be used with the computer network 140 for secure applications as it cannot be copied and it can only be authenticated by the application software 132 communicating with the system server computer 150 and/or web server computer 160. The type 3 RF tag can be read and written to and can be used for performing local applications on the user's network-enabled device without using the computer network 140. For example, the type 3 RF tag can be used to display content such as a business card.

Returning to Figure 4, in block 401, the application software 132 obtains the RF tag 110's unique code sent to it by the RF reader 120. In the decision block 402, the unique code of the RF tag is checked to determine if the type of RF tag is a type 1, type 2 or type 3. If the RF tag is a type 3 RF tag, the application software 132 will begin a local application program on the user computer 130, as shown in block 404. In this embodiment, access via the computer network 140 to a remote server computer is not needed. After completing block 404, the routine 400 loops to checking for another RF tag in the proximity of the RF reader. Alternatively, if the RF tag is either a type 1 RF tag or type 2 RF tag, then the application software 132 obtains the unique code associated with the RF reader 120 as shown in block 406, and proceeds to retrieve a URL from a remote server computer in a method that can be similar to routine 200 depicted in Figure 2.

In addition to different types of RF tag functionality available, various user-interface features can be incorporated into an RF tag and an RF reader. For example, the shape of the RF tag, such as a circle, oval, square, rectangle, triangle, zigzag, etc. can be mode-specific to a particular application. Or LED lights can be incorporated into the RF tag that light-up or flash when the RF tag is in use. Similarly, the RF reader can incorporate lights that illuminate to show when it has been activated, that a transaction is in progress, that an Internet connection has been established, or conversely, that any of the related processes have failed. Sounds can also be incorporated to the RF reader to provide similar indications.

In one aspect of these embodiments, the functionality of the RF reader (read/write capability with respect to the RF tag) can be incorporated into various peripheral devices commonly associated with network-enabled devices. For example, this functionality can be embedded into a mouse controller, a mouse pad, a speaker, a screen monitor, a personal computer, a portable lap top computer, a portable electronic organizer, a digital mobile telephone, a portable audio device, a portable video device, a set-top box, an audio device, a TV-set, or a CD/DVD reader/writer.

Accessories can also be provided to facilitate use of the access system in accordance with the present invention. For example, an RF tag storage device, like an accordion file folder, CD-flip rack, or Rolodex, can be provided to organize the RF tags. An organizer that organizes the RF tags by shape, application, color, date, etc. can also be provided.

Figure 5 is a schematic diagram illustrating encoding of the RF reader 120 with a unique 10-byte identification code in one embodiment. The unique identification code 502 includes a manufacturer's authorization code portion 508, date portion 504, unique ID portion 512, and RF reader type portion 514. The date portion 504 contains day, month, and year fields as illustrated by blocks 504 and 506. The unique identification code 502 is generated and authorized by the system server computer 150 and is registered as "produced, but not in use yet" on the database management component 153 of the system server computer 150. Once an RF reader 120 has been used, the registration field will be changed to "in use." In one aspect of this embodiment, this registration scheme provides a tracking mechanism to prevent unauthorized use of the access system: RF tag readers that

use a registration code that is not produced yet will be unauthorized; and RF readers that use a code that is already in use (*e.g.*, copies) will also be also unauthorized.

Figure 6 is a schematic diagram illustrating the assembly of a unique transaction code 602 ("UTC 602") by the application software 132 in one embodiment. The 160-bit UTC 602 is composed of three unique code portions 604, 606, and 608. The unique reader code portion 604 is associated with the RF reader 120 and contains 80 bits of code. The unique RF tag code portion 606 is associated with the RF tag 110 and contains 64 bits of code. The unique application software code portion 608 contains 16 bits of code that denotes the version of application software 132 that is running on the user computer 130.

Figure 7 is a flow diagram of a routine 700 performed on a server computer for communicating with a network-enabled device in a secure mode in one embodiment. The access system can be performed in secure mode if desired to protect the interests of the parties involved in the transaction being conducted. In one aspect of this embodiment, the routine 700 can run on the system server computer 150 (Figure 1). In other embodiments, the routine 700 can run on the web server computer 160 (Figure 1). In block 701, the routine 700 receives a UTC. Data in the look-up database table 152 of the system server computer 150 corresponding to the UTC indicates that a secure transaction is required, and the routine 700 sets up a secure connection via the computer network 140 (Figure 1), as shown in block 702. A conventional method for setting up a secure connection, known by those of skill in the art, can be used. In block 704, the routine 700 sends an authentication request to the source of the UTC. In response to the authentication request, the routine 700 receives a unique serial number and 32-bit password taken off of the RF tag 110 that initiated the transaction, in block 706. In other embodiments, passwords with more or less than 32 bits can be used. The serial number and password are checked in decision block 708. If the serial number and password do not check out, an error message is returned, as shown in blocks 714 and 716. If the serial number and password do check out, then the routine 700 will look-up and retrieve a URL from the look-up database table 152 corresponding to the UTC received in block 701, as shown in block 710. This URL is then sent along with a new 32-bit password back to the source of the UTC in block 712.

After completing block 712 or 716, routine 700 loops back to block 701 to receive a UTC.

Figure 8 is a flow diagram of a routine 800 performing a secure transaction on a user network-enabled device in one embodiment. In one aspect of this embodiment, the routine 800 can be operating in conjunction with the routine 700 (Figure 7) to receive a URL from a remote server in a secure transaction. In block 801, the routine 800 receives a request for authentication from a server computer. In block 804, the routine 800 sets up a secure connection to the server computer via the computer network 140. In block 806, the routine 800 obtains the unique serial number and 32-bit password of the RF tag 110 using the RF reader 120. The routine 800 then sends the unique serial number and 32-bit password to the server computer via the computer network 140 using the secure connection, as shown in block 808. In block 810, the routine 800 receives an indication from the server computer whether or not the serial number and 32-bit password were authenticated. If the serial number and password were not authenticated, an error message is displayed on the user computer 130 for the user as shown in block 811. If the serial number and password are authenticated, then the routine 800 will receive a new 32-bit password and the desired URL from the server computer, as shown in block 812. The routine 800 then writes the new 32-bit password to the RF tag 110 using the RF reader 120, as shown in block 814. In block 816, the routine 800 launches the browser 134 with the URL received in the secure mode from the server computer. After performing block 816 or 811, routine 800 loops back to block 801 to receive an authentication request from a server.

Figure 9 is a flow diagram of a routine 900 performed by the application software 132 for retrieving information and/or services from a server computer using the access system 100 in an alternate embodiment. In this embodiment, the RF tag is a "simple RF tag" that is encoded with a URL linking the RF tag to a web site that contains the desired information or service. Hence, the user computer 130 does not need to access the system server 150 to obtain the URL of the desired web site. Instead, the application software 132 simply obtains the URL directly from the simple RF tag and uses this URL to launch the browser module 134. In block 902, the routine 900 determines if a simple RF tag is in the proximity of the RF reader 120. In decision block 904, if the simple RF tag is not in

the proximity, the routine 900 continues to check for a tag. If the simple RF tag is in the proximity, the routine 900 obtains the URL from the simple RF tag using the RF reader 120. The routine 900 then launches the browser 134 with the URL to obtain the desired information and/or services from the associated web site, as shown in block 908. After completing block 908, routine 900 loops to block 902 to wait for an RF tag.

A number of alternate embodiments of access system components are possible without departing from the scope or intent of the basic access system. For example, Figure 10 is a schematic diagram illustrating an alternate embodiment of an RF reader code. The standard device descriptor 1002 of the RF reader contains two identification code portions that will describe the device, a two-byte product identification portion 1004, and a two-byte vendor identification portion 1006. The standard device descriptor 1002 will also contain two index code portions, a one-byte manufacturer index code portion 1008 will contain information describing the manufacturer, and a one-byte product index code portion 1010 will contain information about the specific reader. The foregoing alternate reader embodiment can be used in conjunction with a special registration RF tag as explained below.

The access system can use a special registration RF tag to register a user when the user enters the access system for the first time. Figure 11 is a schematic diagram illustrating a data structure 1100 of a registration RF tag in accordance with this embodiment. The data structure 1100 contains an eight-page portion 1102, wherein each page contains 32 bits of information. Page 0 contains a 32-bit serial number portion 1104 of the registration RF tag. Page 3 contains a 32-bit information portion 1110 that includes an eight-bit configuration portion 1111 and a 24-bit password portion 1113. The eight-bit configuration portion 1111 contains a one-bit Manchester code portion 1112, a two-bit RF tag mode portion 1114, a one-bit password mode portion 1116, and four other bits of read and/or write information 1118.

To use the registration RF tag, the user installs the application software on a network-enabled device and connects an RF reader to the network-enabled device. The application software then asks the user to place the registration RF tag in the proximity of the RF reader. After the user has done this, the application software creates a "new user command" to send to the system server

computer. Figure 12 is a schematic diagram illustrating a new user command data structure 1200 in accordance with this embodiment. The new user command data structure 1200 has a 16-bit product identification portion 1202, a 16-bit vendor identification portion 1204, an eight-bit manufacturer information portion 1206, and a 16-bit application software version portion 1208. The 16-bit product identification portion 1202, the 16-bit vendor identification portion 1204, and the eight-bit manufacturer information portion 1206, all come from the code stored on the RF reader and are equivalent to the product identification portion 1004, the vendor identification portion 1006, and the manufacturer information portion 1008, respectively, shown in Figure 10 with respect to the RF reader. The 16-bit software version portion 1208 is provided by the application software. Once the application software has created the new user command data structure 1200, the application software sends this command and 32-bit registration number from the registration RF tag to the system server computer. The registration number of the registration RF tag is the 32-bit serial number portion 1104 of the registration RF tag data structure 1102, as shown in Figure 11.

When the system server computer receives the new user command and the RF tag registration number, it will validate the RF tag registration number and the reader and application software information in the new user command. If the information received by the server computer is validated, the server computer will send a URL of a registration site back to the application software. The application software will then direct a browser program to access the registration site using the URL. The accessed registration application will guide the user through the registration process by directing the user to fill in a web-based screen. In one aspect of this embodiment, the web page will offer three levels of registration to the user: Level 1 will be the minimum required information and will require only the name, gender, birthday, and email address of the user; Level 2 will additionally request the address of the user; and Level 3 will also request the marital status, educational degree, occupation, income, and phone number of the user. Once the user has registered, the server computer will send a confirmation back to the application software. The application software will then locally store the registration RF tag's registration number, which can also be referred to as a "user registration number". When new RF tags are subsequently used with the access system, this user

registration number can be retrieved from local storage for assembly of a unique transaction code (UTC).

In addition to the alternate embodiments of the RF reader and RF tag explained in the foregoing paragraphs, the access system can also include alternate embodiments of the unique transaction code (UTC). In one such alternate embodiment, to begin using the access system, a user will start by placing an appropriate RF tag in the proximity of an RF reader. The RF reader reads the unique code off of the RF tag and sends the RF tag's unique code, and the RF reader's code, to the user's network-enabled device via a wired or wireless connection. The application software running on the user's network-enabled device receives the RF tag's unique code and the reader's code and combines them with the application software version code and, in this alternate embodiment, the user's registration number that has been locally stored on the user's network enabled device, to create a UTC.

Figure 13 is a schematic diagram illustrating the assembly of a UTC 1302 in accordance with the alternate method described in the preceding paragraph. The 128-bit UTC 1302 is composed of four code portions, a 16-bit reader identification portion 1304, a 32-bit user registration number portion 1306, a 64-bit unique RF tag code portion 1308, and a 16-bit application software version code portion 1310. The 16-bit reader identification code portion 1304 comes from the reader code, and is equivalent to the product identification portion 1004 as shown in Figure 10. The user registration number portion 1306 is the 32-bit serial number portion 1104 which originally came from the registration RF tag shown in Figure 11, and is subsequently stored on the user's network enabled device. The unique 64-bit RF tag code portion 1308 is taken from the particular RF tag that happens to be in use.

After creating the UTC, the application software establishes access to the Internet or other suitable computer network and sends the UTC via the network to the system server computer. Using a double look-up table format, the server computer will extract the user registration number 1306 from the UTC and authenticate the user's registration. If the user is validly registered, the server computer will access the second look-up table, extract the RF tag's unique code from the UTC, and compare the RF tag's unique code to the look-up table. The

URL or application associated with the RF tag's unique code is then sent back to the application software. Once the application software receives the URL, the remaining processes for retrieving information or services using this alternate embodiment of the access system can be substantially similar to the processes explained above in accordance with Figures 1-9.

Alternate embodiments also exist for the 64-bit type 1 RF tag and the 256-bit type 2 RF tag discussed above in accordance with Figure 4. For example, Figure 14 is a schematic diagram illustrating the assembly of a unique 64-bit type 1 RF tag data structure 1402 in accordance with one such alternate embodiment. The 64-bit type 1 RF tag has a 40-bit unique code portion 1404 that is arranged in the structure of portion 1406 for use in the UTC. The RF tag code portion 1308 of the UTC shown in Figure 13, however, contains 64 bits of information, not 40. Therefore, there is a 24-bit reserved portion 1408 that is combined with the RF tag code portion 1406 to create the entire 64-bit RF tag code portion 1410 that is used with the UTC.

Figure 15 is a schematic diagram illustrating the assembly of a 256-bit type 2 RF tag data structure 1502 in accordance with an alternate embodiment. The 256-bit type 2 RF tag memory can include 256-bits of EEPROM organized into eight pages 1504 of 32 bits each. The 256-bit RF tag can contain a serial number portion 1512, a password portion 1514, a reserved portion 1516, and a configuration and password portion 1520. The 256-bit RF tag can also contain a unique 64-bit RF tag code portion 1506 on pages 4 and 5 that will be used to create the UTC. The relationship of the eight bytes contained in pages 4 and 5 to the UTC data structure is shown by the relationship portion 1508. Depending on the operation mode and the configuration, pages 6 and 7 can vary. Byte configuration 1530 represents one configuration that can be used for the various bytes of information contained in the data structure 1502. This byte configuration includes a one-bit Manchester code portion 1532, a two-bit RF tag mode portion 1534, a one-bit password mode portion 1536, and four one-bit read and/or write portions 1538. In yet other embodiments, other RF tags with other data structures, memory capacity, and security features may be used to accomplish the same purpose as the type 2 RF tag.

Those of skill in the relevant art will appreciate that the access system disclosed in accordance with Figures 1-15 in its various embodiments can be used

in commercial and non-commercial embodiments to download advertising and other content, perform transactions, or manage data on a computer network such as the Internet. For example, a product seller may offer a free "limited usage" RF tag (*e.g.*, good for three uses) or a free "clipped usage" RF tag (*e.g.*, 60 seconds of an audio track) to distribute audio tracks, movie trailers, or video clips as a method of advertising its product. To view the advertising content in this embodiment, a user places the free RF tag in the proximity of the reader 120. The application software 132 obtains the unique codes off of the free RF tag and the RF reader 120, compiles a UTC, and sends the UTC via the computer network 140 to the system server computer 150. After extracting the free RF tag's unique code from the UTC, the system server computer 150 sends the corresponding URL from the look-up database table 152 to the application software 132. The browser 134 is then launched with this URL, and the advertising content retrieved from the web server 160 with the URL is displayed on the user's network-enabled device for the user to view.

The access system can also be used in a substantially similar manner for pay-per-use sales of audio and video products. In this embodiment, a user can purchase an RF tag permitting the user to download specific audio and/or video content. In one aspect of this embodiment, the RF tag can utilize a secure mode so that unauthorized users cannot access the content. In another embodiment, the access system can be used to facilitate the download of paid-for software on a user's network-enabled device. The user purchases an RF tag from the seller of the online software and uses the RF tag on a network-enabled device to automatically retrieve and download the software that the user purchased. In an embodiment similar to those discussed above, the RF tag could be used to provide the user access to peer-to-peer networks. The RF tag in these embodiments can be enabled with a decrementing device that decrements the number of uses of the RF tag. The RF tag can also include a display component that displays how many times the RF tag has been used to download the content, and/or how many more times the tag can be used.

Radio content can also be accessed using the access system disclosed herein. In this embodiment, a special RF tag is used that accesses the appropriate radio content on a server computer and plays the audio content on the user's

network-enabled device. In this embodiment, a user can listen to Internet radio stations using his or her own personal presets stored on the system server computer independent of the location of the user or the kind of network-enabled device being used. In addition, special radio station RF tags can locate and store new and interesting radio stations and programs.

Various methods can be employed to distribute the different RF tags used in the access system. For example, an RF tag vending machine or an RF tag kiosk can be located in various public places or stores for dispensing the RF tags to purchaser/users. These RF tags can be pre-encoded with unique codes linking them to various URLs and other resources, such that purchasers/users can select from the RF tags according to which tag provides the service, information, or content desired. Alternatively, the kiosk or vending machine can provide a system that enables the purchaser/user to personalize the RF tag by recording user specific links and other personal presets for the RF tag in the system server computer.

In addition, "Blank" RF tags can also be stocked that are not yet printed with the various attributes that permit different types of network access. The vending machine or kiosk can be fitted with an RF tag read/write device so that a personalized user interface with personal presets can be encoded onto the RF tag by the user/purchaser. The vending machine can also be fitted with a camera, keyboard and/or microphone to further personalize the RF tag with personal audio recordings, a photograph, or a picture or video linked to the RF tag. After the user selects the desired attributes of the RF tag, and the payment and transaction is confirmed by the system server computer, the combination of the unique RF code and the selected attributes are embedded in the RF tag and the vending machine/kiosk will print the RF tag with appropriate graphics and distribute it to the user/purchaser.

Payment for the various RF tags sold or dispensed through the vending machine or kiosk can be done either online (credit card, banking card) or offline (smart card, banking card or an RF tag prepaid debit card). When the RF tag is paid for, the system server computer will store the link between the user's payment data and the unique RF tag identification code as a method for authenticating the user when the RF tag is subsequently used.

In an alternate embodiment of the access system, shops, museums, and other establishments can be fitted with RF readers near products or venues of interest. When a selected RF tag is placed on such an RF reader, the information on the particular product or venue is stored on the system server computer's look-up database under the unique RF code of that particular RF tag. Later, the user can use the RF tag on any network-enabled device to access and display the product or venue information, to compare products, or take another (interactive) look at that museum exhibit at leisure.

Unlinked RF tags are also available in an embodiment of the access system. This RF tag initially has no link to any application, URL, or transaction on the system server computer. Via a special service performed by the system server computer, a user can link the RF tag to specific content like a web site, piece of music, greeting card, picture, or movie. In this embodiment, instead of sending the application software a URL, the system server computer recognizes the RF tag's code as being one that is unlinked, and sends the user a request via the application software to visit a specific URL to make the desired links on the currently unlinked RF tag. Alternatively, the system server computer could send the application software a request to provide the linking desired by the user. After entry by the user, this desired linking is then written to the RF tag by the RF reader. This service allows a user to immediately access the desired links anywhere that the user uses the RF tag. The personal links established by the user on the previously unlinked RF tag can also be edited subsequent to the initial linking to change the content or service accessed by the RF tag.

The access system can also be used to store and categorize various data for a user or a business in another embodiment. In one aspect of this embodiment, the data of interest can be stored in a system server computer database under a unique RF code. When an RF tag with that unique code is used on a network-enabled device, the data will be immediately retrieved. The system can be used to store details on an employee, medical patient, or other selected person to be recalled by the user independent of the location or network-enabled device used. This information can be used for security purposes, personnel records, or for personal information like gaming levels, stock portfolios, or frequently and/or last used phone numbers. Similarly, the system can be used as a file/directory

management device. Instead of searching archaic records and old electronic files, or trying to remember the file name that the document was saved under, business or personal documents can be linked with an RF tag for easy access and document management without having to go through the arduous task of finding a particular storage site.

The access system can also be used to reduce on-time departure problems in public transit systems that may result from passengers not being aware of current departure status. For example, if a passenger is given a boarding pass that includes an RF tag, the passenger can use the RF tag at various kiosks located within a terminal to easily obtain current departure information. This relieves the passenger of relying on a public address system to obtain a change of departure information.

The access system can also be used to create a user's personalized computing environment regardless of the remote network-enabled device that the user happens to be located at. The personalized computing office or information of the user is stored on the system server computer, and an RF tag is used to retrieve and display this personalized data on a remote network-enabled device. For example, if the user is using a network-enabled device in a shared or rented office space, an RF tag can be encoded with personalized computer environment settings that can include choice of language, personal data like address books, and email addresses and software applications. The RF tag can also be used to provide the user with access to personal applications when using a remote network-enabled device.

Those of ordinary skill in the relevant art will appreciate that the access system can also facilitate advertising over a computer network in various embodiments. For example, a company can distribute free RF tags to users whereby placing the RF tag in the presence of an RF reader takes the user directly to the target advertising information the company wants the user to see. Similarly, the RF tag can be used to provide the user with almost instant access to an advertiser's on-line product catalogue. In this way, the user can research and compare the product in the comfort of the user's own home on his or her own time. The RF tags distributed to consumer users with direct links to advertising web sites can also include information directing the user to the nearest branch or outlet that

sells the advertised products. The free RF tags can also permit recipient users to retrieve and download freeware onto the user network-enabled devices, wherein the content of the freeware contains advertising related to the company's products.

As an adjunct to the advertising function, the access system can also be used as a business card. Instead of distributing paper business cards, a businessperson can create and distribute RF tag "business cards" to clients. When placed in the proximity of a reader, the businessperson's contact details and email address will immediately be displayed to the client. This RF tag embodiment can convey a great deal more information to the client than could be included on an ordinary business card. A pre-addressed email screen could also be displayed that would allow the client to contact the business person by simply typing a message and pressing "send."

Those of skill in the relevant art will also appreciate that the access system disclosed herein can be employed as a useful resource-locating tool. For example, an RF tag can be included when a user purchases a particular product. If needed later, the user can use the RF tag to bring up details on the product such as service information, specifications, safety records, logistics, user manuals, parts and service catalogs, or shipping and tracking information. In addition, this information can be linked to online purchases of other related items. Similarly, the RF tag can be linked to direct customer service support whenever the user has problems and/or questions regarding the product or service. Warranty registration can also be facilitated with the access system by using an RF tag to identify a product or service and allowing the purchaser of the product or service to perform the warranty registration procedures online with the RF tag from the purchaser's own network-enabled device.

The RF tag can be used for product sales documentation in a substantially similar manner. For example, an RF tag can be written with extra information at the point of purchase so that the product manufacturer, purchase date, purchase amount, sales outlets and other purchase specifics can be linked to the RF tag and stored on the system server computer. This guarantees that the customer always has access to the correct purchase information, product updates, frequently asked questions, etc. The point of purchase can also be fitted with an RF

tag printer to further personalize the RF tag with pertinent purchase and/or product information.

In addition to the useful functions outlined above, the access system can also provide useful authorization functions for Internet or other computer network-related transactions. For example, financial institutions (banks, brokers, e-commerce payment systems) can use the RF tag to confirm authorization for online payments or to access other paid-for online services, by using one of the secured embodiments discussed above. The RF tag can also be used to authorize an online email system, or as a prepaid debit card. In one aspect of this embodiment, an RF tag can be purchased with a value amount (*e.g.*, in time, money, number of accesses, etc.) which can be deducted upon authorization. This amount can be stored on the RF tag itself or on the system server computer. The RF tag can be fitted with a small display that displays the amount of value left either on the RF tag itself or on a network-enabled device. In a further authorization embodiment, an RF tag can be used with the access system as a gambling device that acts as a debit card that automatically deducts or adds credit to a gambler's account.

The access system can also be used as a purchasing tool in alternate embodiments. For example, online services such as magazine subscriptions, market research, etc., can be purchased by a user by purchasing an RF tag that is linked to the selected content. The system can also be used to make Internet phone calls using a familiar user interface and personal presets independent of the location of the user or the kind of network-enabled device being used, by storing the user interface and presets on the system server computer and accessing them with an RF tag. Similarly, the access system can be used to make videoconference calls using a familiar user interface with personal presets. The system can also be used by communication companies to offer a complete personalized phone or videoconference service using the RF tag as a calling card.

The access system can also be used as a global positioning system (GPS) guide that directs a user to businesses and other services in one embodiment. In this embodiment, the RF tag's unique code will direct the system server computer to send the user's network-enabled device the parameters of the location the user desires to go to. The user's network-enabled device can then use these parameters along with the current location parameters of the user (acquired from a typical GPS

system) to provide the user with directions to the desired location – for example, a store, restaurant, or other service provider.

In yet another embodiment, the access system can be used to distribute coupons or other product information to a store customer. In one aspect of this embodiment, the customer could present an RF tag to an RF reader upon entering the store, or an RF tag carried on the customer's person could be automatically read by an RF reader as the customer enters the store. Alternatively, the RF tag could be read as the customer approaches selected products within the store. Either way, in response to receiving the RF tag's unique code, the server computer can cause a telephone call or page to be placed to the customer's cell phone that audibly displays product coupons or other product information to the customer. Alternatively, the server computer can cause paper coupons to be automatically printed-out for the customer to pick up at a kiosk located within the store.

As part of the manufacturing of the access system components, the RF reader 120 will be acceptance tested by an RF reader test unit. The RF reader 120 can be connected to this test unit with a USB connector. The test unit will check the hardware functionality, and a test RF tag will be used to make contact with the system server computer 150. The system server computer 150 will register a new RF reader code and send this new unique RF reader code to the RF reader's programmable memory via the test unit. The unique code associated with this particular RF reader 120 will then be stored on the database component of the server computer 150. The test unit will have secure connection to the server computer 150. Both the RF reader test unit and the test RF tag will be part of a manufacturing package that can be licensed to manufacturers of the access system components described in accordance with Figure 1.

Many aspects of the embodiments discussed above are also described in enabling detail in the "Chippo System Specification for Personal Computer Systems," version 0.73, dated July 5, 2000, which is included herein as Appendix A. From the foregoing it will be appreciated that although specific embodiments of the access system have been described for purposes of illustration, various modifications may be made without deviating from the spirit and scope of the invention. Accordingly, the invention is not limited except by the appended claims.

APPENDIX A

Chippo System Specification
for Personal Computer Systems

Version 0.73
July 05, 2000

Chippo System Specification For Personal Computer Systems

1. Document objective and revision history

Objective of the document
This document specifies the Chippo System for Personal Computer environments. The specification describes PC Software attributes, Server applications, the protocol definition, types of transactions, types of Chippo tokens and Database setup. This specification is to be seen as a User Requirement Specification. It is intended that this specification will be accompanied by a Technical Requirement Specification.

Revision history
Version 1.3 - March 17, 2000
Includes secure transaction process and UTC definition.

Version 1.4 - May 26, 2000
Includes server applications and updated CHAPP - Server protocol.

Version 0.7 - June 23, 2000
Includes changes in the user registration process and reader identification resulting in several changes throughout the document. Updated UTC definition and CHAPP - Server protocol. Versioning is brought in line with other documents: <1.0 is not final.

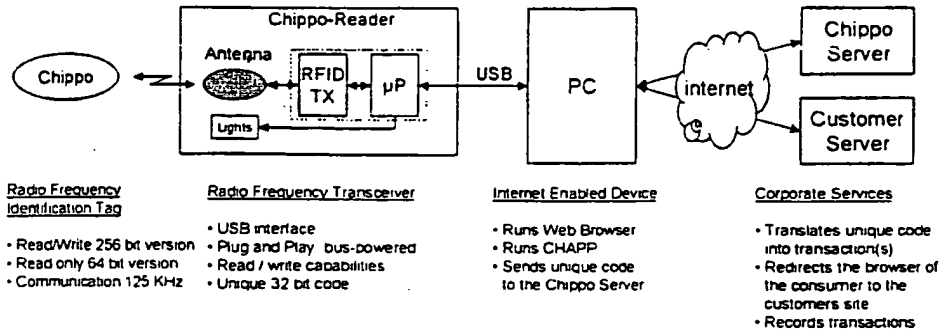
Version 0.71 - June 27, 2000
User registration process changed.
Registration Chippo added. Change in idProduct of the reader.

Version 0.73 - July 05, 2000
All flow charts updated.

Future updates will include detailed User Interface dialogs

2. System Architecture and Components overview

The Chippo system allows users to shortcut and simplify their Internet activities by eliminating the need to remember, type, or mouse click to a website or server. The users simply throws the Chippo on to the Chippo Reader, and the Chippo Application Software, via an Internet or network enabled device, will take the user directly to the desired website or server without the hassle of typing, clicking or memorizing an URL address. The diagram below depicts the Chippo system and its main components.



The Chippo system consists of 4 main building blocks and 2 enabling blocks.

Building blocks:

- Chippo Token
- Chippo Reader
- CHAPP Software
- Chippo Server + Software

Customer Server + Software Enabling blocks:

- Personal Computer (PC)
- Internet connection

3. System Requirements

Personal Computer:

- Internet Connection
- Web Browser (Internet Explorer 5, Netscape 5, or later)
- Free USB port
- CDROM Drive
- Windows 98 or Windows2000

4. Chippo Reader

The Chippo Reader will connect to the PC via USB.
It will connect to the USB host as a Human Input Device (HID Class).

In the standard device descriptor 2 ID codes of 2 bytes each will describe the device:

- **idProduct**
  Defined by Chippo Technologies
- **idVendor**
  Defined by the USB Implementers Forum

In the standard device descriptor 2 index codes of 1 byte each will point to information about the manufacturer of the reader and product specific information:

- **iManufacturer**
  Will point to a string descriptor describing the manufacturer
  The string will be 1 byte allowing 256 different manufacturers
- **iProduct**
  Will point to a string descriptor containing product specific information, this will include the full part number of 5 Bytes (hex-dec). The full content of the string is to be defined

5. Chippo Token

Chippo tokens come in three different versions: the 64-bit version, the 256-bit version and the 2048-bit version.
In this document Chippo Tokens are also referred to as "Chippos".

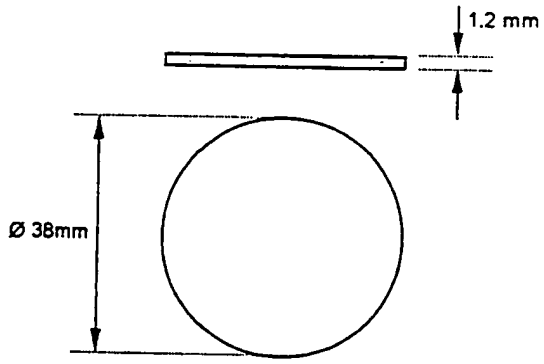
The 64 bit Chippos are mainly used for non-secure applications like advertising, samplers of Audio/Video, greeting cards, etc

The 256 bit Chippos are used for applications that require security. These Chippos can not be copied and can be authenticated by the CHAPP software and the applications running on the Chippo server and the customer server.

The 2048 bit Chippos will be used to distribute data for off-line use like business cards. The specification of these Chippos is not part of this document.

Chippo Specification				
Memory	Type	RO/RW	Password	Off-line use
64	1	RO	No	No
256	2	RW	Yes	No
2048	3	RW	No	Yes
bits				

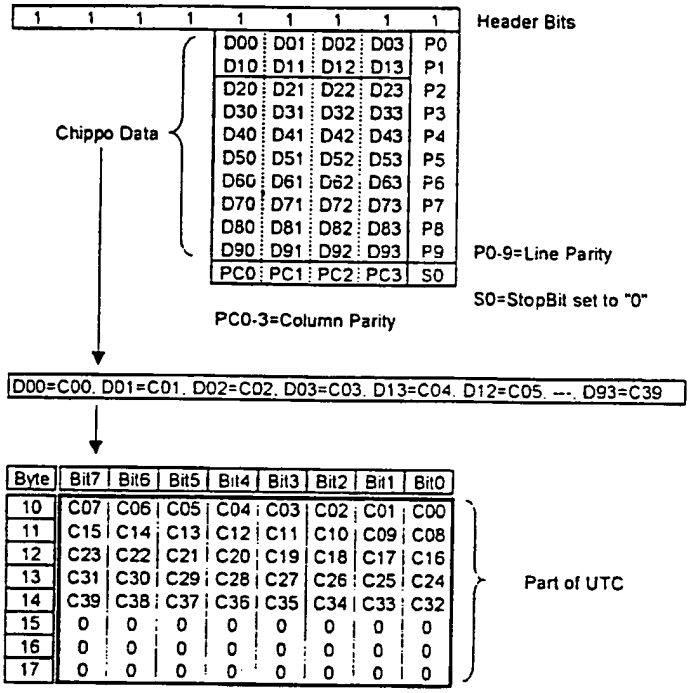
Type 1 and type 2 Chippo dimensions:



5.1. Chippo - 64 Bit

The 64 bit Chippo has a 40 bits unique code, allowing 240 = 1,099,511,627,776 unique codes.

The data structure of the 64Bit read-only Chippo and translation to the UTC:



The Chippo data of 40 bits will be part of the Unique Transaction Code (UTC) that will be sent to the Chippo Server. The 16 remaining bits reserved in the UTC for Chippo info will be set to "0" (Byte 15 - 17).

Coding of the 40 bits will be decided on a per case basis. The coding of the 64 bit Chippos will be agreed with the supplier. A separate document will specify the rules for protecting these codes.

5.2. Chippo - 256 Bit

The 256 bit Chippo has a 64 bits unique code,
allowing 264 = 18,446,744,073,709,551,616 unique codes.

The memory of this Chippo consists of 256 bits EEPROM and is organized in 8 pages of 32 bits each. Depending on the operation mode the configuration of these pages and the content of Pages 4-7 can differ.

Page	Content
0	Serial Number
1	Password RWD
2	reserved
3	8 bit Config and 24 bit Password
4	Chippo Data
5	
6	
7	

The 256 Bit Chippo can operate in different modes for the different applications.
The present Chippo applications will use the following configuration setting:

Configuration Byte 256bit applications								
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	
0	1	1	0	0	1	1	0	66

- Manchester Code
- Hitag 2 mode
- Password mode
- Page 6 and 7 Read/Write
- Page 4 and 5 Read Only
- Page 3 Read Only
- Page 1 and 2 Read/Write

Page 4 and 5 contain the code that will be part of the UTC to be sent to the Chippo Server. The translation is as follows:

Chippo				
Page 4:	Byte 3	Byte 2	Byte 1	Byte 0
Page 5:	Byte 7	Byte 6	Byte 5	Byte 4

Chippo	UTC
Byte 0	Byte 10
Byte 1	Byte 11
Byte 2	Byte 12
Byte 3	Byte 13
Byte 4	Byte 14
Byte 5	Byte 15
Byte 6	Byte 16
Byte 7	Byte 17

6. CHAPP-Server Communicati n Prot col

CHAPP will communicate with the server to send and receive commands.

The CHAPP software and the server software will use the following commands:

- CHIPPO START <CHAPP to Server>
- TRANSACTION START <Server to CHAPP>
- CHIPPO STOP <CHAPP to Server>
- TRANSACTION STOP <Server to CHAPP>
- NEW USER <CHAPP to Server>
- USER REGISTRATION <Server to CHAPP>
- AD POP-UP <Server to CHAPP>

CHIPPO START (CHAPP to Server)

CHAPP will send the Unique Transaction Code (UTC) of 136 bits containing 4 codes plus parameters to the Chippo Server:

- 16 bit Reader ID code (= idProduct)
- 32 bit User registration number
- 64 Bit code of the Chippo
- 16 Bit CHAPP Version

Parameters:

- CHAPP indicates that this a "start": this means that the Chippo has just been put on the reader

The Unique Transaction Code (UTC):

Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	
0	P07	P06	P05	P04	P03	P02	P01	P00	Reader ID (=idProduct)
1	P15	P14	P13	P12	P11	P10	P09	P08	
2	R07	R06	R05	R04	R03	R02	R01	R00	User registration #
3	R15	R14	R13	R12	R11	R10	R09	R08	
4	R23	R22	R21	R20	R19	R18	R17	R16	
5	R31	R30	R29	R28	R27	R26	R25	R24	
6	C07	C06	C05	C04	C03	C02	C01	C00	Chippo Code
7	C15	C14	C13	C12	C11	C10	C09	C08	
8	C23	C22	C21	C20	C19	C18	C17	C16	
9	C31	C30	C29	C28	C27	C26	C25	C24	
10	C39	C38	C37	C36	C35	C34	C33	C32	
11	C47	C46	C45	C44	C43	C42	C41	C40	
12	C55	C54	C53	C52	C51	C50	C49	C48	
13	C63	C62	C61	C60	C59	C58	C57	C56	
14	V07	V06	V05	V04	V03	V02	V01	V00	CHAPP Version
15	V15	V14	V13	V12	V11	V10	V09	V08	

TRANSACTION START (Server to CHAPP)

The Server will send a URL plus parameters to the CHAPP software

Parameters:

- Field indicating that there is a "STOP" transaction. This means that CHAPP has to send a CHIPPO STOP code once the Chippo is removed from the reader

CHIPPO STOP (CHAPP to Server)

The CHIPPO STOP command will be send to the Chippo server if it was requested by the server in the parameters of the TRANSACTION START command. CHAPP will send the Unique Transaction Code (UTC) of 128 Bits containing 4 codes plus parameters to the Chippo Server:

- 16 bit Reader ID code
- 32 bit User registration number
- 64 Bit code of the Chippo
- 16 Bit CHAPP Version

Parameters:

- CHAPP indicates that this a "stop": this means that the Chippo has just been removed from the reader

TRANSACTION STOP (Server to CHAPP)

The Server will send this command to CHAPP once it has received the CHIPPO STOP command. The command includes a URL (www.chippo.com) and a parameter byte.

NEW USER (CHAPP to Server)

Once CHAPP is installed and a reader is connected for the first time, CHAPP will ask the user to put on the registration Chippo. CHAPP will read the User Registration Number from the Chippo and send the <New User> command to the server comprising the data below. The server will respond with the "user registration" command.

Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	
0	P07	P06	P05	P04	P03	P02	P01	P00	idProduct
1	P15	P14	P13	P12	P11	P10	P09	P08	
2	V07	V06	V05	V04	V03	V02	V01	V00	idVendor
3	V15	V14	V13	V12	V11	V10	V09	V08	
4	M07	M06	M05	M04	M03	M02	M01	M00	iManufacturer
5	A07	A06	A05	A04	A03	A02	A01	A00	CHAPP Version
6	A15	A14	A13	A12	A11	A10	A09	A08	

CHAPP will await the confirmation by the server and once received it will store the user registration number on the PC's HDD for use in all future UTCs.

USER REGISTRATION (Server to CHAPP)

Once the "new user" command is received the server will check the validity of the reader information, the CHAPP version and the user registration number.
The user registration number is the unique 32 bits serial number of the Hitag2 Chippo.

The server will send back the URL of the Chippo Reader Registration site.

Here the registration application will guide the user through the registration process. See Chapter 9.4 Registration Application.

When OK the server will send back the "User Registration" command as a confirmation to CHAPP. CHAPP can now locally store the user registration number.

AD POP-UP (Server to CHAPP)

The Server will send a URL plus parameters to the CHAPP software

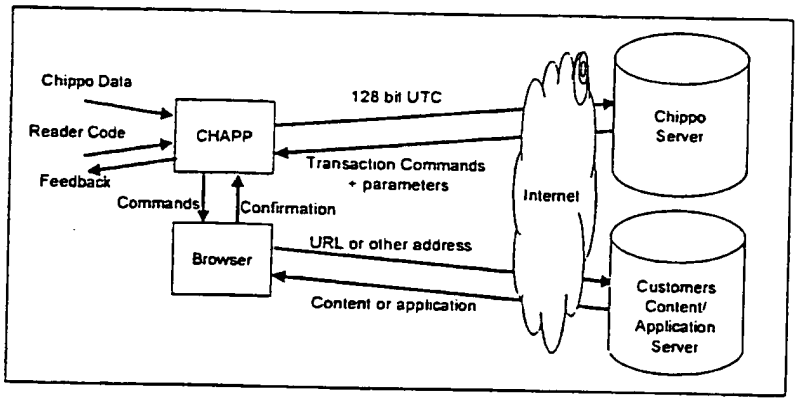
Parameters:

- Field to indicate this is a pop-up ad URL

7. Chippo Application Software (CHAPP)

Functional requirements CHAPP:

1. Sends 128-bit UTC to the server (see flowchart for transactions) once a Chippo is put on the reader
2. Sends (on request of the server) a Chippo stop command to indicate that a Chippo was removed from the reader
3. Generates an "active icon" in the Windows Taskbar
4. Generates error messages in case of malfunction or use of an unauthorized Chippo or Chippo Reader
5. Instructs the Browser to display certain website(s)
6. User can specify preferred browser program (Netscape or IE)
7. Handles secure authentication requests from the customers application
8. Reads and writes passwords on the Chippo



7.1. CHAPP Functionality

The next six flowcharts show the basic functionality of the CHAPP program.

1. <CHIPPO START>, CHAPP to Server.
Once a Chippo is put on the reader CHAPP will read the Chippo code from the token and create the UTC by getting the stored User Registration Number, the Chippo Reader Code (is idProduct) and the version of the CHAPP Software. This will be sent to the server.

2. <TRANSACTION START>, Server to CHAPP.
The server will send back a URL and a parameter byte. CHAPP will start the browser (if not already running) and will give an indication on the reader via the LED's.

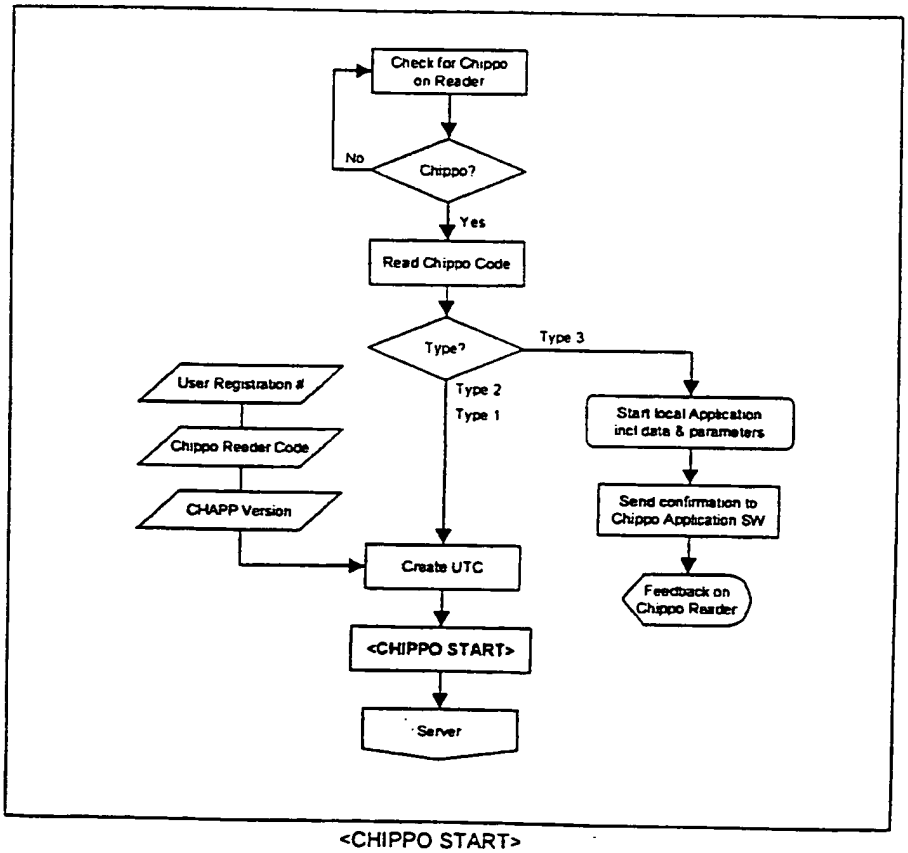
<CHIPPO STOP>, CHAPP to Server.
CHAPP will send the UTC + parameters indicating this is a Stop command to the Chippo Server once a Chippo is being removed from the reader. CHAPP will only do this if this was requested by the Server in the <TRANSACTION START> command.

3. <TRANSACTION STOP>, Server to CHAPP.
The Server will send this command to CHAPP once it has received the CHIPPO STOP command. The command includes a URL (www.chippo.com) and a parameter byte.

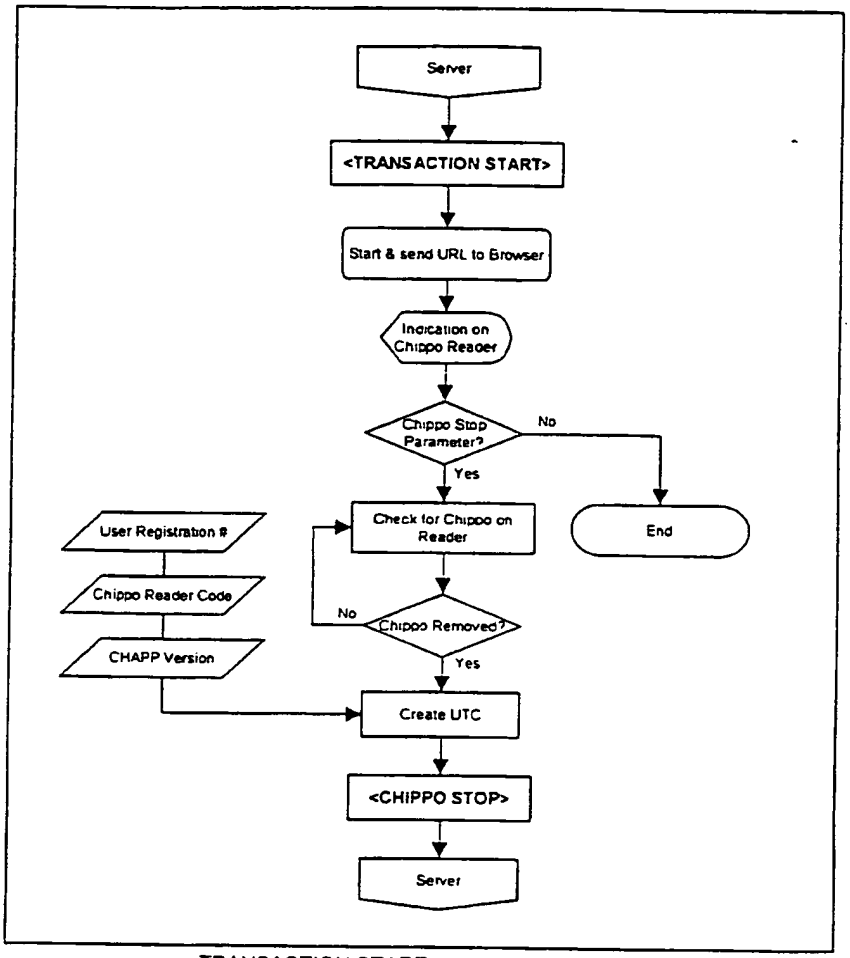
4. <NEW USER>, CHAPP to Server.
Once CHAPP is installed and a reader is connected for the first time and a user has put the registration Chippo on the reader, CHAPP will send a <NEW USER> command to the server. The server will respond with the <USER REGISTRATION> command. CHAPP will await the confirmation by the server and once received it will store the user registration number on the PC's HDD for use in all future UTCs.

5. <USER REGISTRATION>, Server to CHAPP
Once the <NEW USER> command is received the server will check the validity of the reader information, the CHAPP version and the user registration number. The server will send back the URL of the Chippo Reader Registration site. Here the registration application will guide the user through the registration process. See Chapter 8.3 User Registration Information.
When OK the server will send back the <USER REGISTRATION> command as a confirmation to CHAPP. CHAPP can now locally store the user registration number.

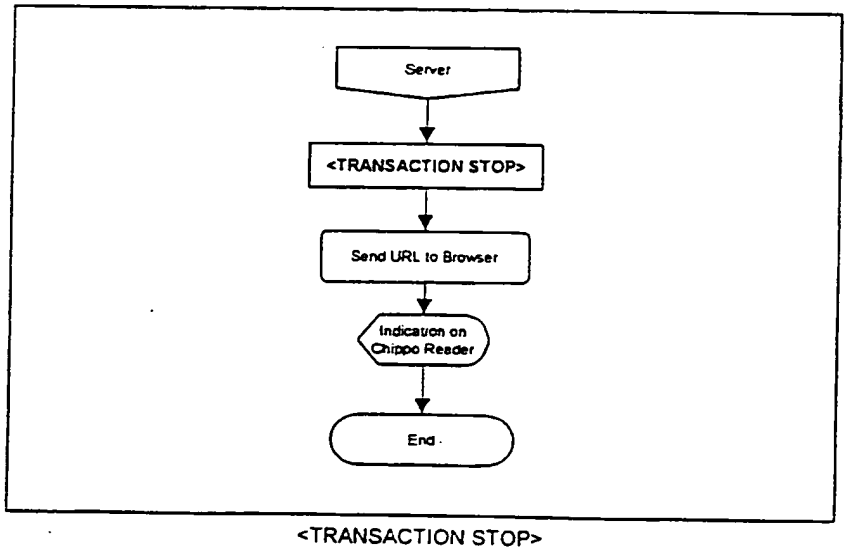
6. <AD POP-UP>, Server to CHAPP
The Server will send a URL plus parameters to the CHAPP software with a field to indicate this is a pop-up ad URL. The ad should appear on top of the other windows.



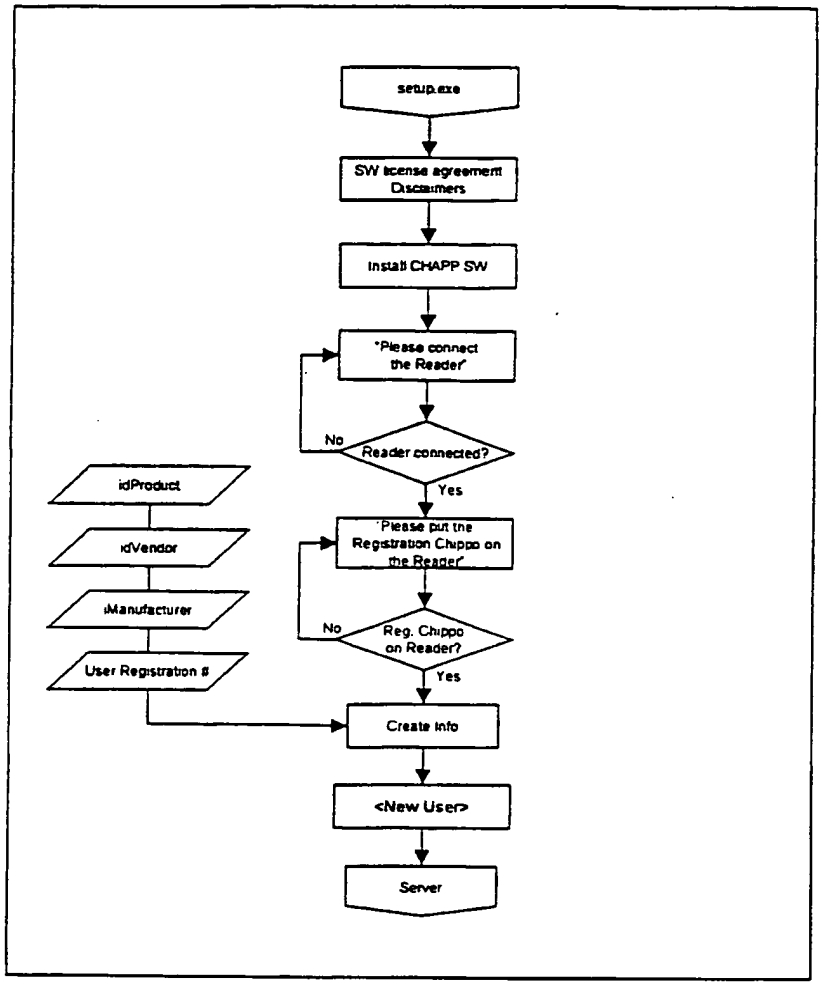
<CHIPPO START>



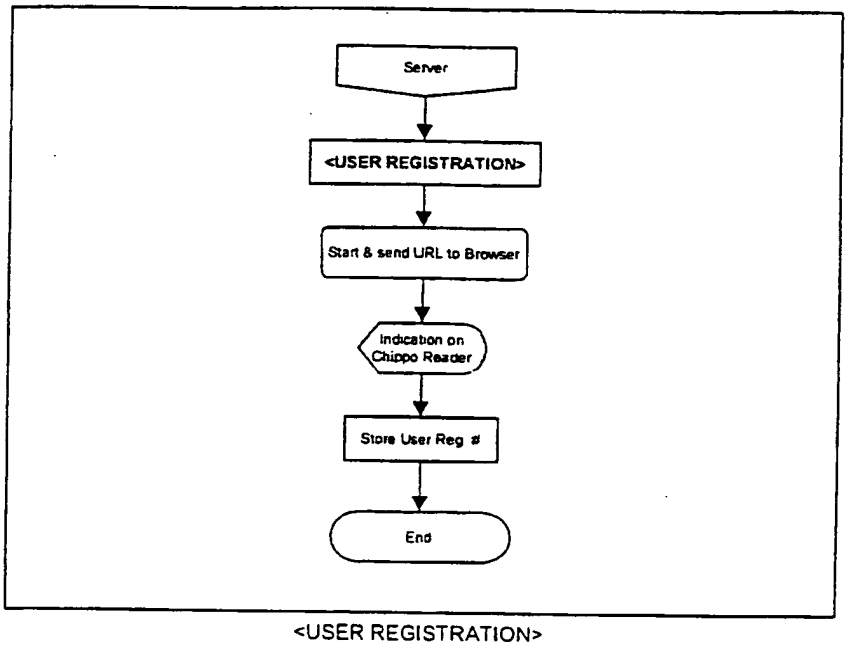
<TRANSACTION START> & <CHIPPO STOP>



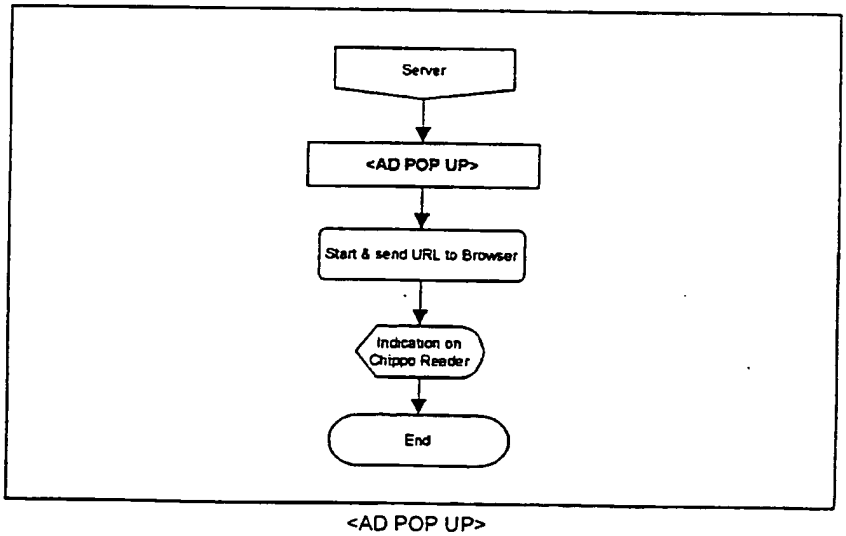
<TRANSACTION STOP>


setup.exe
SW license agreement Disclaimers
Install CHAPP SW
'Please connect the Reader'
No
Reader connected?
Yes
idProduct
idVendor
iManufacturer
User Registration #
'Please put the Registration Chippo on the Reader'
No
Reg. Chippo on Reader?
Yes
Create Info
<New User>
Server

<NEW USER>



<USER REGISTRATION>



<AD POP UP>

7.2. CHAPP User Interface

When the CHAPP logo on the Windows taskbar is double clicked CHAPP will display a window containing the following buttons:

- Update CHAPP Software
- Update registration
- Information:
- CHAPP Version
- Legal Information

7.3. CHAPP Installation

CHAPP will be installed from a CDROM, this CDROM contains:

- setup.exe Installs the CHAPP Software
- readme.txt Gives installation information

During the installation a number of setup screens will be displayed like the SW license agreement (to be defined). Once installed the software will be started and CHAPP will check for a connected reader and will ask for the registration Chippo to be put on the reader. It will get the 32 bits unique code from the registration Chippo and will get the reader code from the reader and will send this to the server using the "New User" command (see Chapter 7.).

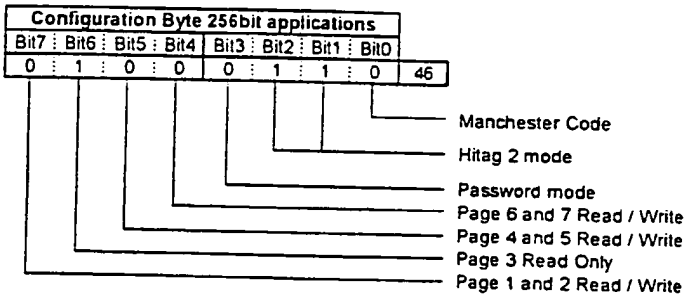
7.4. Registration Chippo

The registration Chippo is used when registering yourself as a new user or when you want to change/update your registration info. It will also provide entrance to the Chippo.com site for personalized services.

The registration Chippo is a 256 bit (Philips Hitag2) Chippo.
The serial number in page 0 of the tag will be used as the user's registration number.
The memory map of the registration Chippo:

Page	Content
0	Serial Number
1	Password RWD
2	reserved
3	8 bit Config and 24 bit Password
4	reserved for future use
5	
6	
7	

The configuration byte of the registration Chippo:



Pages 4 to 7 will contain the following code when delivered to the user:

Location	HEX value
Page 4:	FF – FF – FF – FF
Page 5:	FF – FF – FF – FF
Page 6:	FF – FF – FF – FF
Page 7:	FF – FF – FF – FF

8. Chippo Server

8.1. Chippo Server Architecture

The Chippo Server Architecture contains two main Databases:

- Look-up table
- Chippo Database

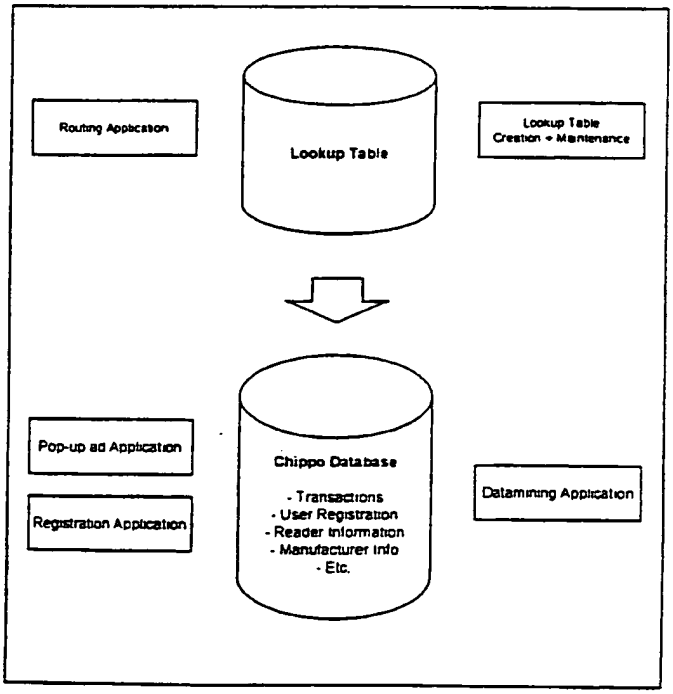
Around these databases a number of applications are running:

- Routing Application
- Pop-up advertising Application

Customer synchronization Application

- User Registration Application + Reader validity check
- Datamining Application + Customer website

Chippo Server Architecture:

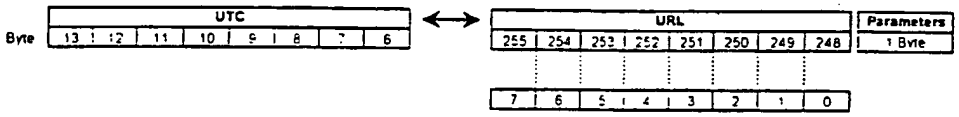


8.2. Routing Application and Look-up table

The Routing application main functions:

- Matches part of the UTC (Unique Transaction Code) it receives from CHAPP with a specific URL in the Lookup Table
- Check the Chippo Reader and Chippo codes on validity
- Create the parameter byte
- Sends the corresponding transaction (URL + parameter byte) back to the CHAPP that originated the UTC
- Sends the transactions to the Chippo Database

Look-up Table contents:



Parameters:
0 : Reserved
1 : This transaction needs to be stopped when the Chippo is removed
2 : The URL is a pop-up ad
3 : CHAPP version needs to be updated
4 : UTC was not valid
5 : Password Chippo
6 : ....
|
|
255 : ....

The performance of the Routing Application and the Look-up table is of high importance: they determine the speed with which the consumer's browser is redirected to the corresponding web site.

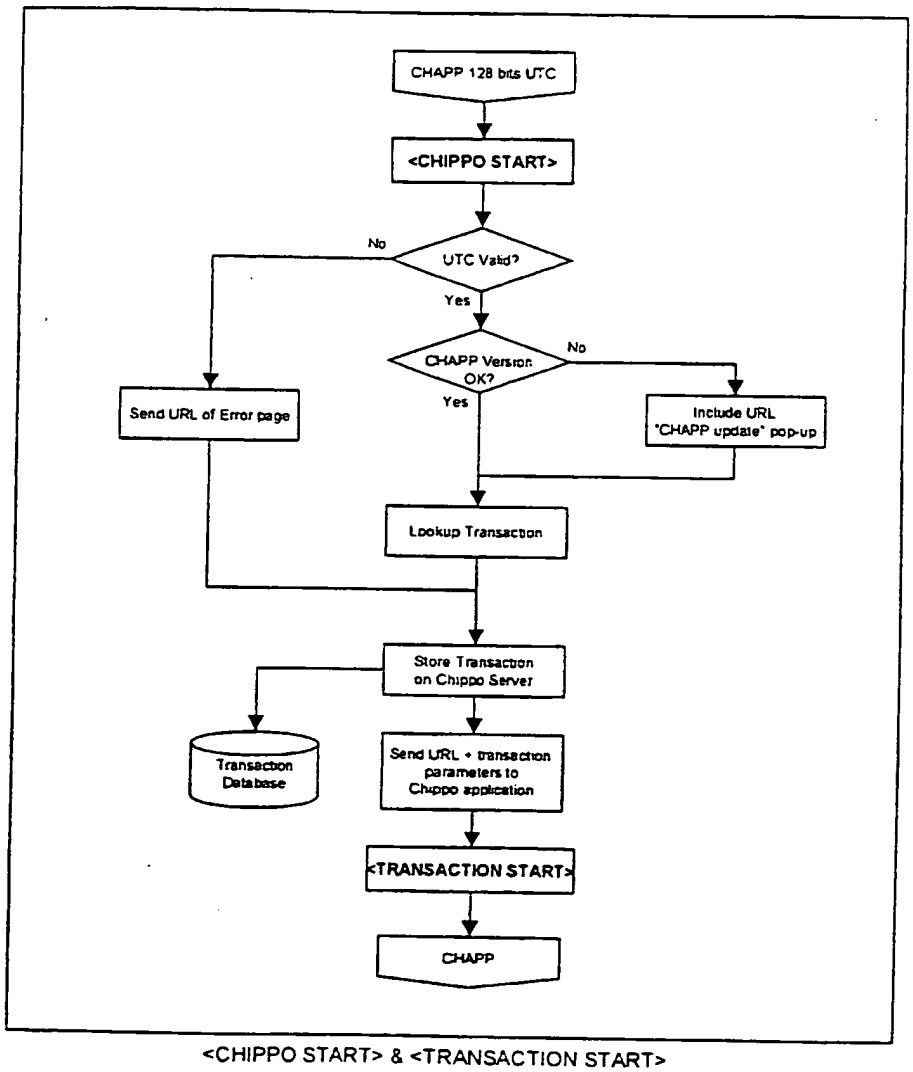
The functionality of the server application is explained below.

1. <CHIPPO START>, CHAPP to Server.
Once a Chippo is put on the reader CHAPP will create and send the UTC to the server. The routing application will lookup the URL and the parameters that correspond to the UTC. This will be sent back to CHAPP via the <TRANSACTION START>, Server to CHAPP, command.

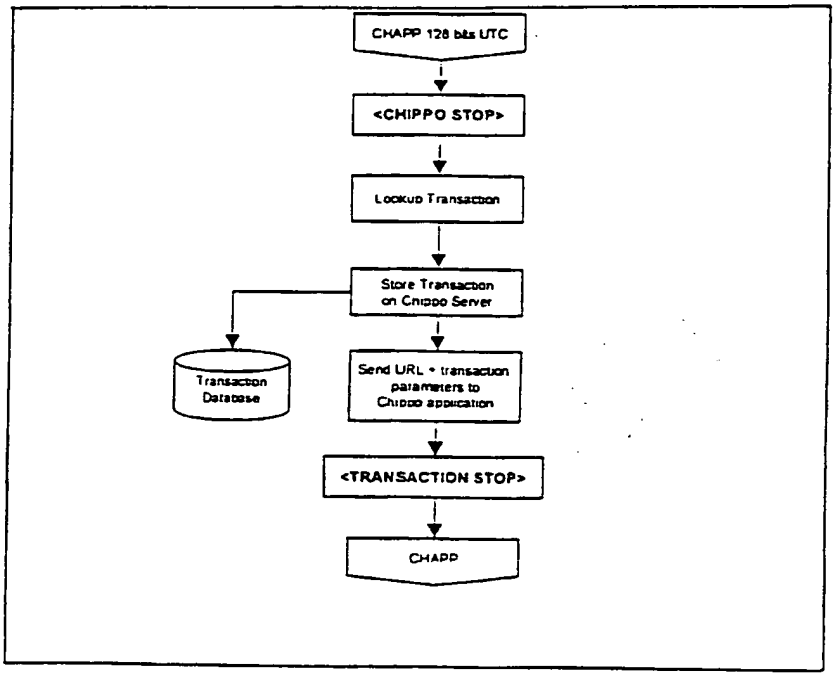
2. <TRANSACTION STOP>, Server to CHAPP.
The Server will send this command to CHAPP once it has received the <CHIPPO STOP> command. The command includes the www.chippo.com URL and a parameter byte.

3. <USER REGISTRATION>, Server to CHAPP
Once the <NEW USER> command is received from CHAPP the server will check the validity of the reader information, the CHAPP version and the user registration number. The server will send back the URL of the Chippo Reader Registration site. Here the registration application will guide the user through the registration process. See Chapter 8.3 User Registration Information.
When OK the server will send back the <USER REGISTRATION> command as a confirmation to CHAPP. CHAPP can now locally store the user registration number.

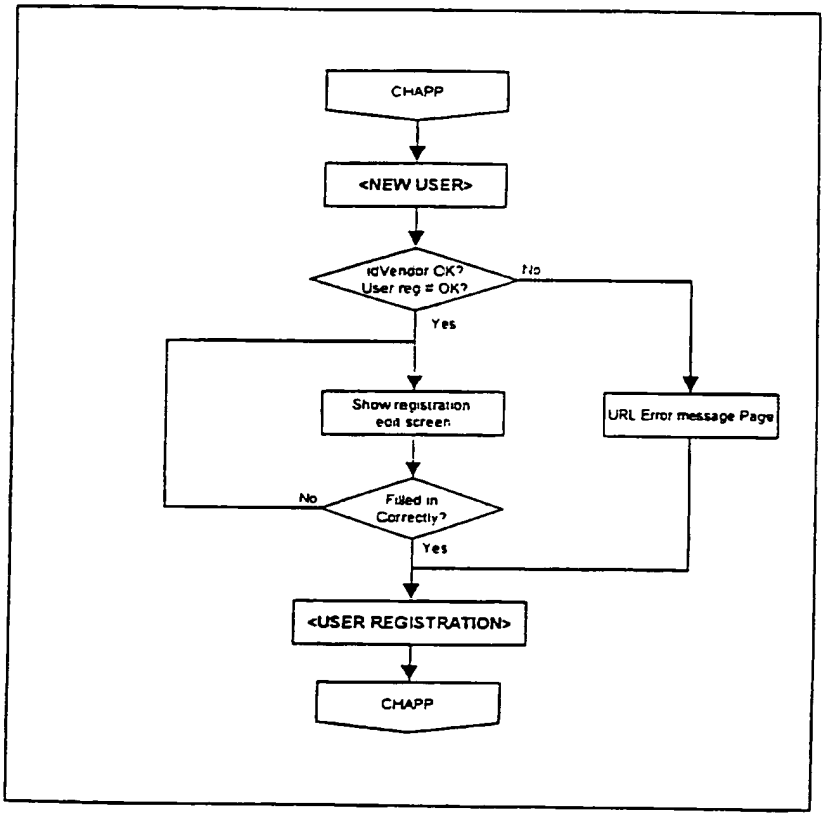
4. <AD POP-UP>, Server to CHAPP
The Server will send a URL plus parameters to the CHAPP software with a field to indicate this is a pop-up ad URL. The ad should appear on top of the other windows.



<CHIPPO START> & <TRANSACTION START>



<CHIPPO STOP> & <TRANSACTION STOP>



<NEW USER> & <USER REGISTRATION>

8.3. The Chippo Database

Transaction information

The Chippo Database keeps a log file that contains all transactions done with Chippos. Combined with the User Registration Information this provides an enormous amount of usage information.

Datafields in the Chippo Database:

1. UTC
   - Reader ID
   - User Registration Number
   - Chippo Code
   - CHAPP version in use
2. Time & Date of transaction
3. IP Address of the PC running the CHAPP

User Registration Information

The User Registration Application registers users during the CHAPP & reader installation process by filling in a web-based screen. It will receive 9 bytes from CHAPP describing the idProduct, idVendor, iManufacturer and the 32 bits user registration number. The application will check if the idVendor and the user registration number are valid. The idVendor is a fixed code linked to Chippo Technologies and issued by the USB IF. The User Registration Number is a unique 32 bits code generated by Philips Semiconductors. The code received from CHAPP should be in between two values that we will receive Philips. Once checked by the server CHAPP will store the user registration number on the PC's HDD. On the server the registration information is stored in the Chippo Database.
The web application will gather the following information to be stored in the Chippo Database. The web page will offer three levels of registration:

Level 1 - minimum required information:

First Name
Last Name
Gender
Birthday
E-mail address

Level 2 (please fill in this information to receive Chippos in the mail - please also check your name above to correspond with the mailing address)

Address
State
ZIP
Country

Level 3 (if you want to do us a favor)

Marital status (yes/no/MBA)
Degree
Occupation
Income
Phone Number
Favorite color

The database will store some other Chippo related information as well:

32 bits User Registration Number
Date of registration
Modify date
Reader ID

8.4. Pop-up Advertising Application

To be defined in Version 1.1

On the basis of reader usage stored in the Chippo Database the pop-up advertising application can send a specific transaction command to CHAPP. CHAPP will re-direct the browser to display an advertising frame on top of the Browser's main screen. See CHAPP-Server Communication Protocol.

Example:

8.5. Lookup Table Creation & Maintenance Application

To be defined in Version 1.1

8.6. Datamining Application + Customer website

To be defined in Version 1.1

9. Manufacturing & Security

9.1. Reader Manufacturing Pr cess

In the standard device descriptor 2 ID codes of 2 bytes each will describe the device:
idProduct : part number 0 - 65536
idVendor : defined by the USB Implementers Forum, is a fixed code

In the standard device descriptor 2 index codes of 1 byte each will point to information about the manufacturer of the reader and product specific information:
iManufacturer : will point to a string descriptor describing the manufacturer
the string will be 1 byte allowing 256 different manufacturers
iProduct : will point to a string descriptor containing product specific information, this will include the full part number of 5 Bytes (hex-dec). The full content of the string is to be defined

Once the Chippo Reader is produced it will be tested at the end of the line by our CRM-unit (Chippo Reader Manufacturing unit). The Reader will be hooked up to the CRM by the USB connector. The CRM will check the hardware functionality and will check the standard device descriptor.
In a later stage (2001) a Manufacturing Authorization Chippo Token will be used to make contact with the Chippo Server. The server will authenticate the Chippo Token and the Chippo Reader. The CRM will have a secure connection to the Chippo Server. Both the CRM and the Manufacturing Chippo will be part of the manufacturing package and potential licensing package.

9.2. Security

The user registration system will provide protection on two levels:

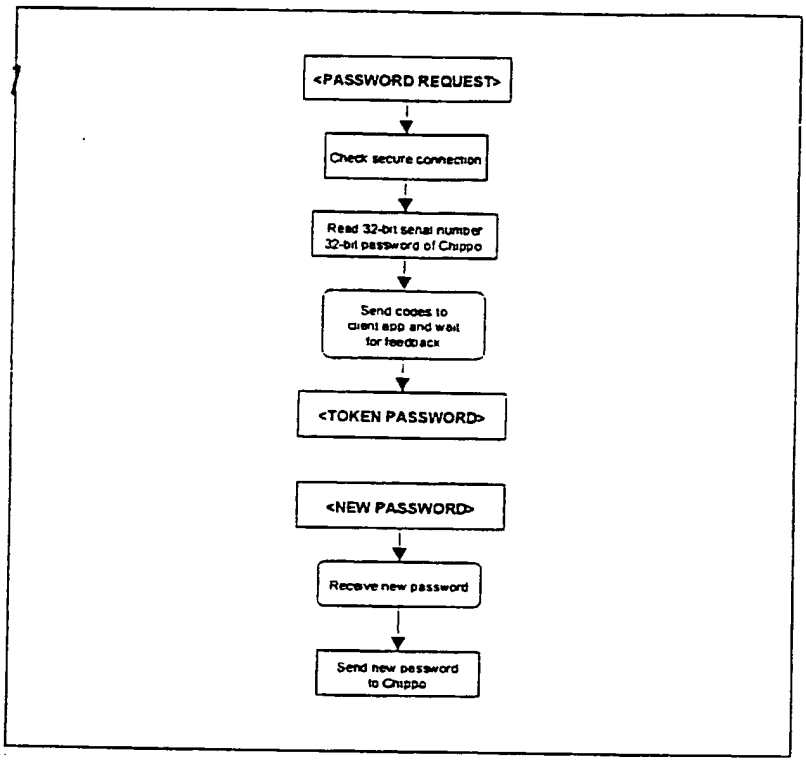
1. The idVendor which is stored in the USB Reader is provided by the USB Implementers Forum (USB IF). This will put manufacturers which copy readers including our idVendor code in conflict with the USB IF. When the copy product uses a different idVendor code it will not be accepted by our servers during the registration process.

2. The User Registration Number is identical to the serial number of the User Registration Chippo token. This number is issued by Philips Semiconductors. Copies of these tokens and/or their unique serial numbers will be in conflict with Philips Semiconductors.

10. Secure Chippo system

CHAPP Secure Authenticati n.

For secure authentication of Chippos the customer application will request the Chippo serial number and password from CHAPP. CHAPP will send this to the customer application and as a response CHAPP will receive back a new password which needs to be written to the Chippo.

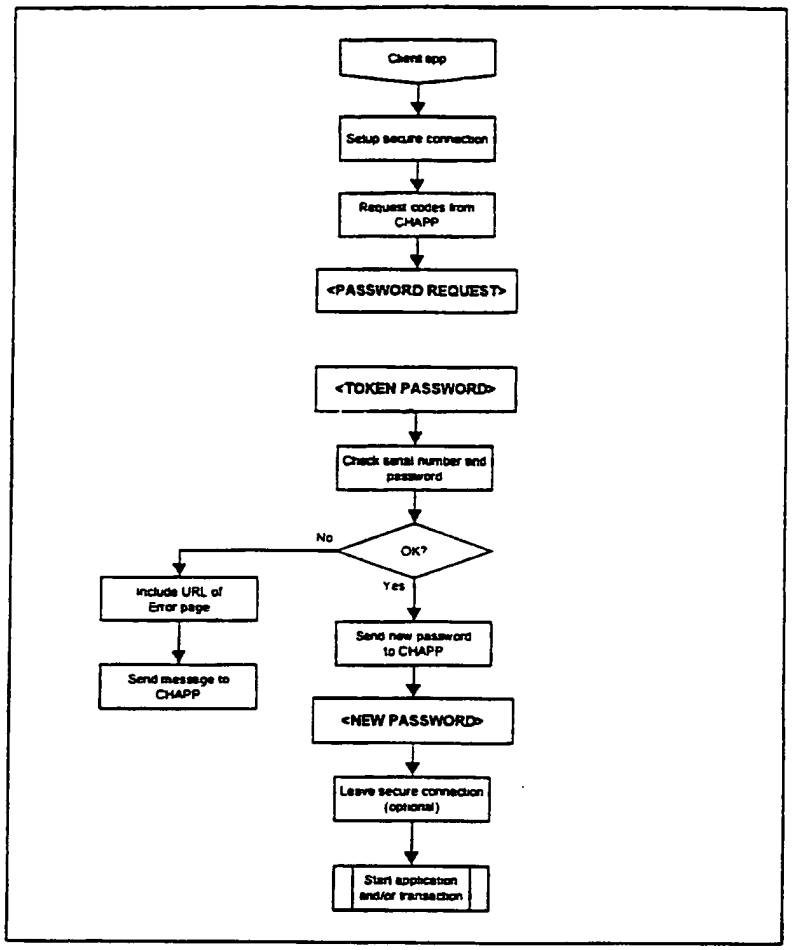


CHAPP Secure Authentication

Customer\Server Secure Authentication application:

At the customer side the server can authenticate the Chippo by two means:
1. The unique 32 bits serial number
2. A password check

The customer server sets up a secure connection to the consumers PC (e.g. via SSL). Upon request of the customer server the CHAPP software will deliver the 32-bit unique serial number and the 32-bit password recorded on the Chippo to the customer application (customer app). Once authenticated the customer app will send back to CHAPP the new password to be recorded on the Chippo and the transaction can take place.



Customer Application for Secure Authentication

11. Related Documents

Philips Semiconductors	Hitag Transponders Rev. 1.2	February 1999
EM Microelectronic Marin	H4100 Product Sheet Rev B/189	1997

CLAIMS

We Claim:

1. A computer-based method for providing access to resources, the method comprising:

encoding a computer-readable medium with a code;

storing the code in a database table of a server computer that links the code to selected data;

distributing the computer-readable medium to a user;

when the user places the computer-readable medium in the proximity of a reader device, reading the code off of the computer-readable medium, and transmitting the code to a user computer;

sending the code from the user computer to the server computer;

receiving the code by the server computer;

retrieving the selected data linked to the code in the database table; and

sending the selected data to the user computer.

2. The method of claim 1 wherein the selected data sent to the user computer is a uniform resource locator for information and/or services content, and wherein the method further comprises:

launching a browser program on the user computer with the uniform resource locator;

retrieving the content associated with the uniform resource locator; and

providing the content to the user computer.

3. The method of claim 1 wherein encoding a computer-readable medium with a code comprises encoding a radio-frequency identification device

with a radio-frequency identification code, and wherein reading the code off of the computer-readable medium includes reading the radio-frequency code with a radio-frequency reader device that transmits the radio-frequency identification code to the user computer.

4. A computer-readable medium containing a data structure comprising:

a product identification code portion;

a vendor identification code portion;

a manufacturer index code portion; and

a product index code portion.

5. The computer-readable medium of claim 4 wherein the product identification code portion contains 16 bits of information.

6. The computer-readable medium of claim 4 wherein the vendor identification code portion contains 16 bits of information.

7. The computer-readable medium of claim 4 wherein the manufacturer index code portion contains 8 bits of information.

8. The computer-readable medium of claim 4 wherein the product index code portion contains 8 bits of information.

9. A method in a server computer system for transmitting data to a user computer system, the method comprising:

providing a mapping of each of a plurality of codes and corresponding resource identifiers;

receiving from the user computer system one of the plurality of codes, the received code being obtained by the user computer system from a computer-readable medium supplied by a user;

identifying the resource identifier that corresponds to the received code based on the mapping; and

sending the identified resource identifier to the user computer system so that the user computer system can present to the user the resource identified by the resource identifier.

10. The method of claim 9 wherein the resource is a web page.

11. The method of claim 9 wherein the resource identifier is a uniform resource locator.

12. The method of claim 9 wherein the resource is an identifier of a computer file on a computer network.

13. The method of claim 9 including receiving from the user computer system another code that identifies the user computer system.

14. A computer-based method for allowing users to access a web page, the method comprising:

reading a code from a computer-readable medium when the user places the computer-readable medium in the proximity of a reading device;

sending the read code to a server computer system;

in response to sending the read code, receiving a resource identifier for the web page from the server computer system;

retrieving the web page identified by the received resource identifier; and

presenting the retrieved web page to the user.

15. The method of claim 14 wherein the device that performs the reading of the code from the computer-readable medium includes an identifier and wherein the sending includes sending the identifier associated with reader device.

16. The method of claim 14 wherein the server computer system uses the received code to select a web page.

17. A computer-based method of advertising comprising distributing, to users who are to view an advertisement, a computer-readable medium identifying the advertisement so that when the computer-readable medium is read by a computer system, the computer system automatically retrieves the advertisement and displays it to the user.

18. A method in a server computer system for transmitting data to a user computer system, the method comprising:

providing a mapping of at least one code and corresponding selected data;

receiving from the user computer system at least one of the codes, the received code being obtained by the user computer system from a computer-readable medium supplied by a user;

identifying the selected data that corresponds to the received code based on the mapping; and

sending the selected data to the user computer system.

19. The method of claim 18 wherein the selected data is a web page.

20. The method of claim 18 wherein the selected data is a uniform resource locator.

21. The method of claim 18 wherein the selected data is an application program.

22. The method of claim 18 wherein the selected data is an identifier of a computer file on a computer network.

23. A computer-based method for allowing users to access web pages, the method comprising:

reading a code from a computer-readable medium when the user places the computer-readable medium in the proximity of a reading device;

sending the read code to a server computer system;

in response to sending the read code, receiving the web page associated with the read code; and

displaying the received web page.

24. The method of claim 23 including before receiving the web page and in response to sending the read code, receiving an identifier of the web page and sending the identifier to a web server system wherein the web page is received from the web server system.

25. A computer-readable medium containing a data structure comprising:

a 32 bit serial number portion;

a 32 bit password portion; and

a 32 bit information portion consisting of an 8 bit configuration portion and a 24 bit password portion.

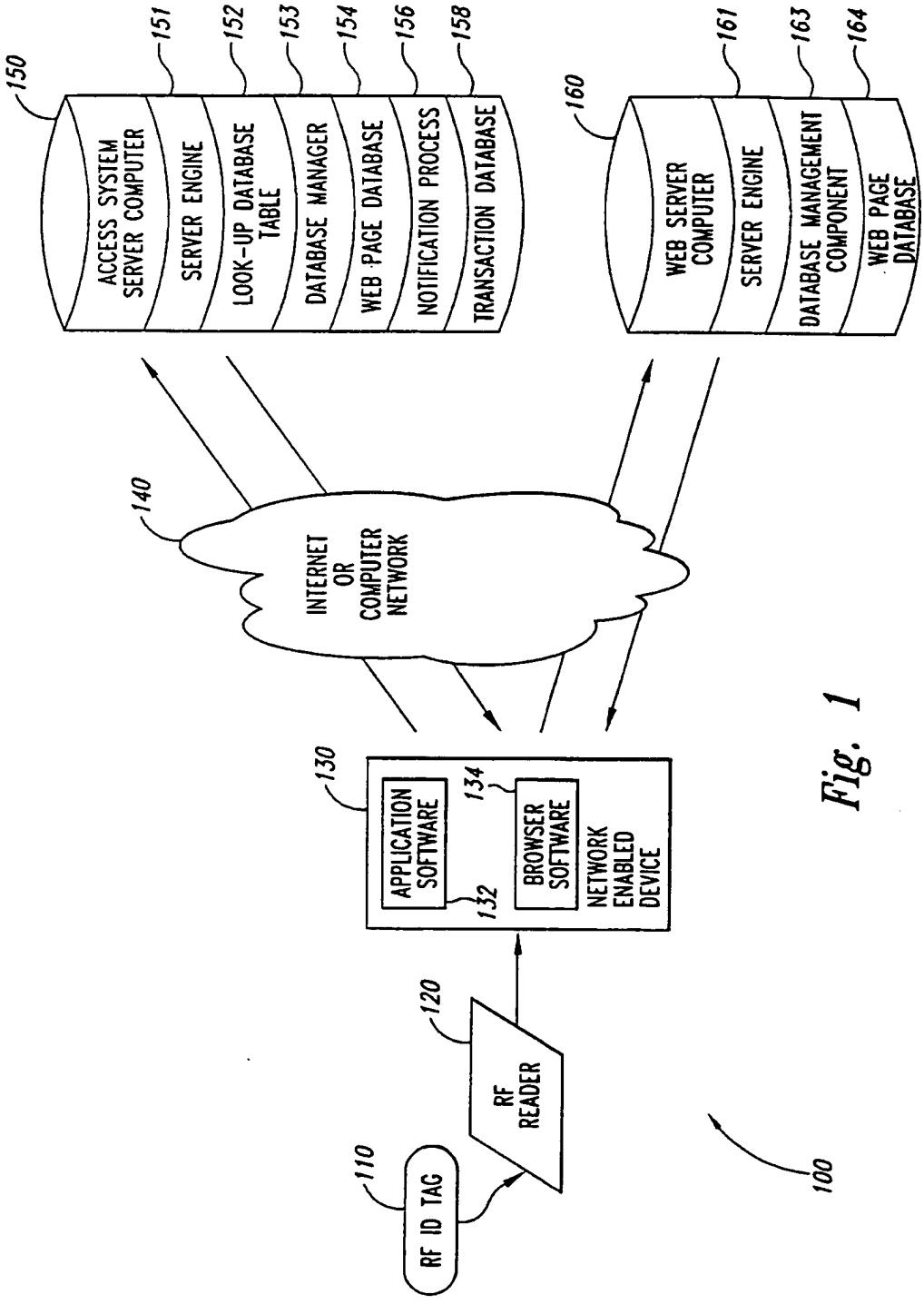

150
151
152
153
154
156
158
ACCESS SYSTEM SERVER COMPUTER
SERVER ENGINE
LOOK-UP DATABASE TABLE
DATABASE MANAGER
WEB PAGE DATABASE
NOTIFICATION PROCESS
TRANSACTION DATABASE
160
161
163
164
WEB SERVER COMPUTER
SERVER ENGINE
DATABASE MANAGEMENT COMPONENT
WEB PAGE DATABASE
140
INTERNET OR COMPUTER NETWORK
130
APPLICATION SOFTWARE
132
134
BROWSER SOFTWARE
NETWORK ENABLED DEVICE
120
RF READER
110
RF ID TAG
100

Fig. 1

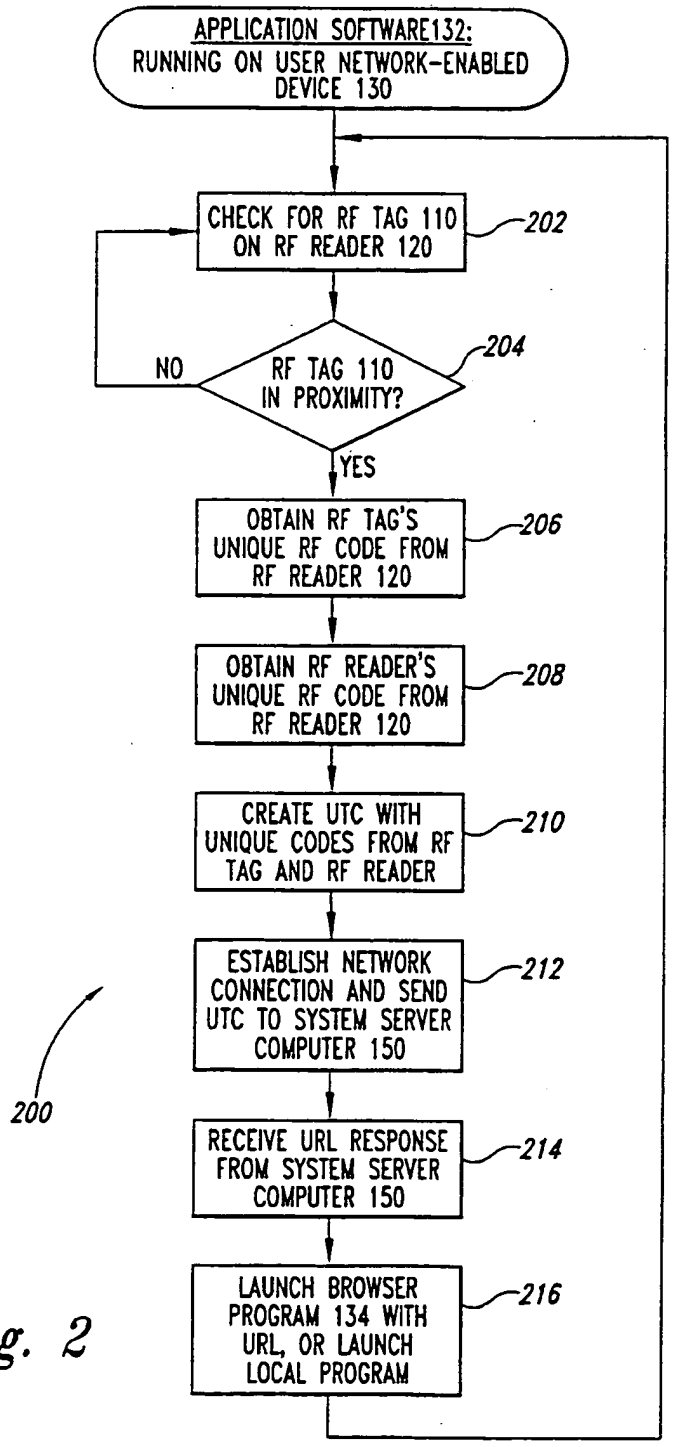

APPLICATION SOFTWARE132: RUNNING ON USER NETWORK-ENABLED DEVICE 130
CHECK FOR RF TAG 110 ON RF READER 120
202
RF TAG 110 IN PROXIMITY?
204
NO
YES
OBTAIN RF TAG'S UNIQUE RF CODE FROM RF READER 120
206
OBTAIN RF READER'S UNIQUE RF CODE FROM RF READER 120
208
CREATE UTC WITH UNIQUE CODES FROM RF TAG AND RF READER
210
ESTABLISH NETWORK CONNECTION AND SEND UTC TO SYSTEM SERVER COMPUTER 150
212
RECEIVE URL RESPONSE FROM SYSTEM SERVER COMPUTER 150
214
LAUNCH BROWSER PROGRAM 134 WITH URL, OR LAUNCH LOCAL PROGRAM
216
200

Fig. 2

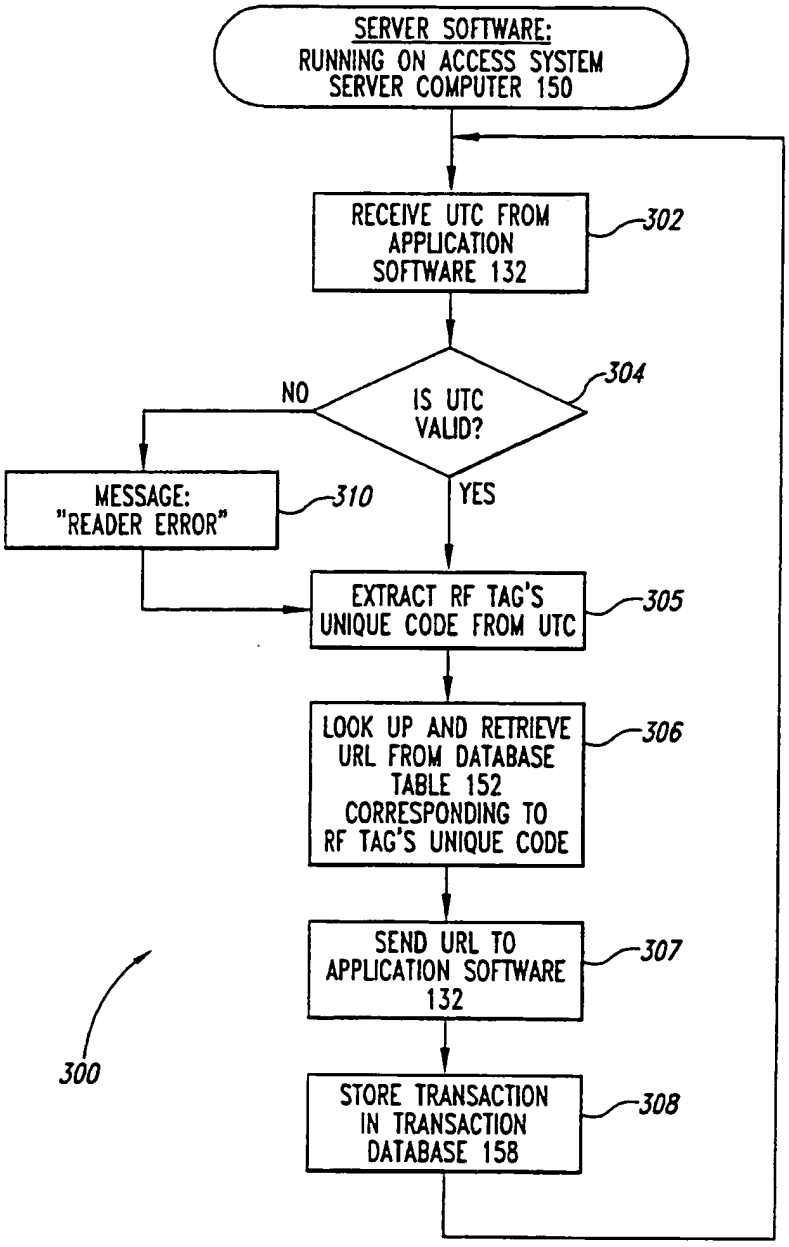

SERVER SOFTWARE:
RUNNING ON ACCESS SYSTEM SERVER COMPUTER 150
RECEIVE UTC FROM APPLICATION SOFTWARE 132
302
IS UTC VALID?
304
NO
YES
MESSAGE: "READER ERROR"
310
EXTRACT RF TAG'S UNIQUE CODE FROM UTC
305
LOOK UP AND RETRIEVE URL FROM DATABASE TABLE 152 CORRESPONDING TO RF TAG'S UNIQUE CODE
306
SEND URL TO APPLICATION SOFTWARE 132
307
STORE TRANSACTION IN TRANSACTION DATABASE 158
308
300

Fig. 3

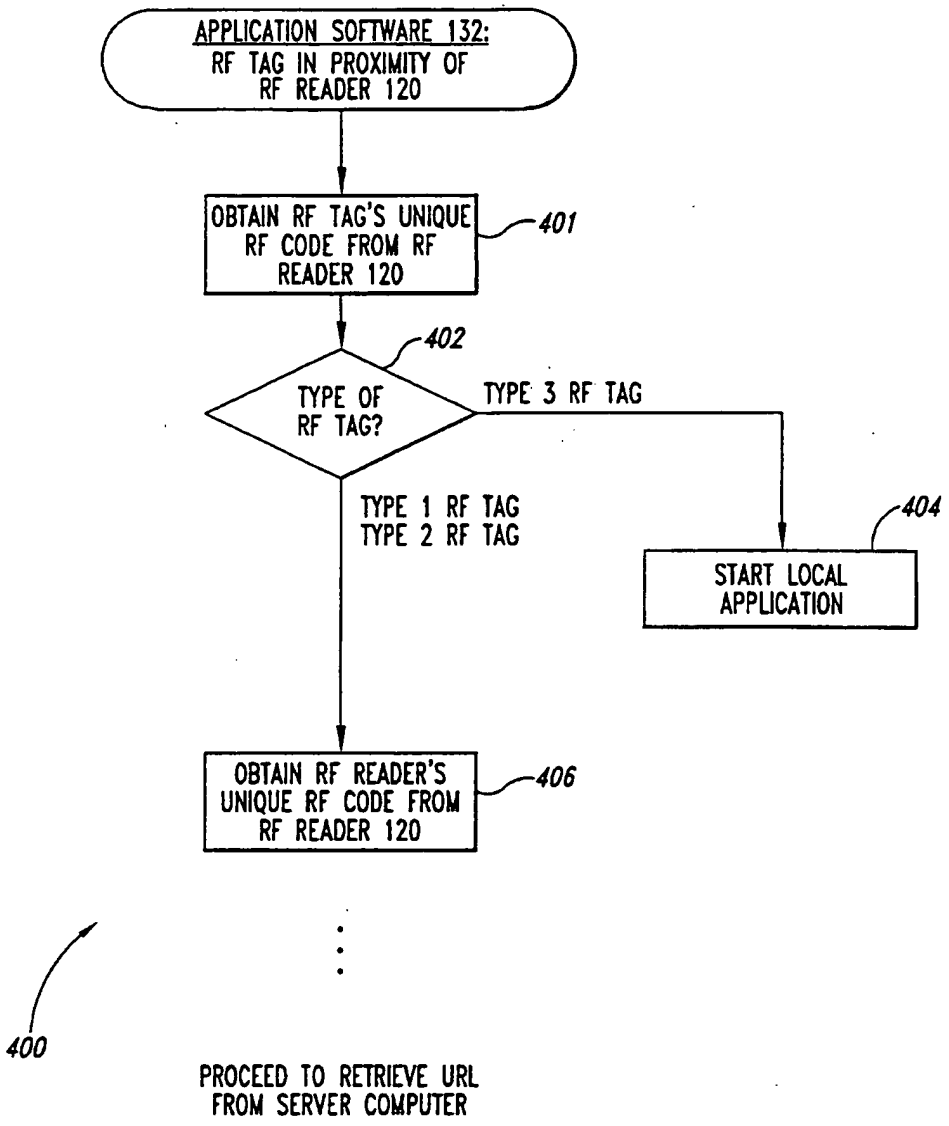

APPLICATION SOFTWARE 132:
RF TAG IN PROXIMITY OF RF READER 120
OBTAIN RF TAG'S UNIQUE RF CODE FROM RF READER 120
401
402
TYPE OF RF TAG?
TYPE 3 RF TAG
TYPE 1 RF TAG
TYPE 2 RF TAG
404
START LOCAL APPLICATION
OBTAIN RF READER'S UNIQUE RF CODE FROM RF READER 120
406
400
PROCEED TO RETRIEVE URL FROM SERVER COMPUTER

Fig. 4

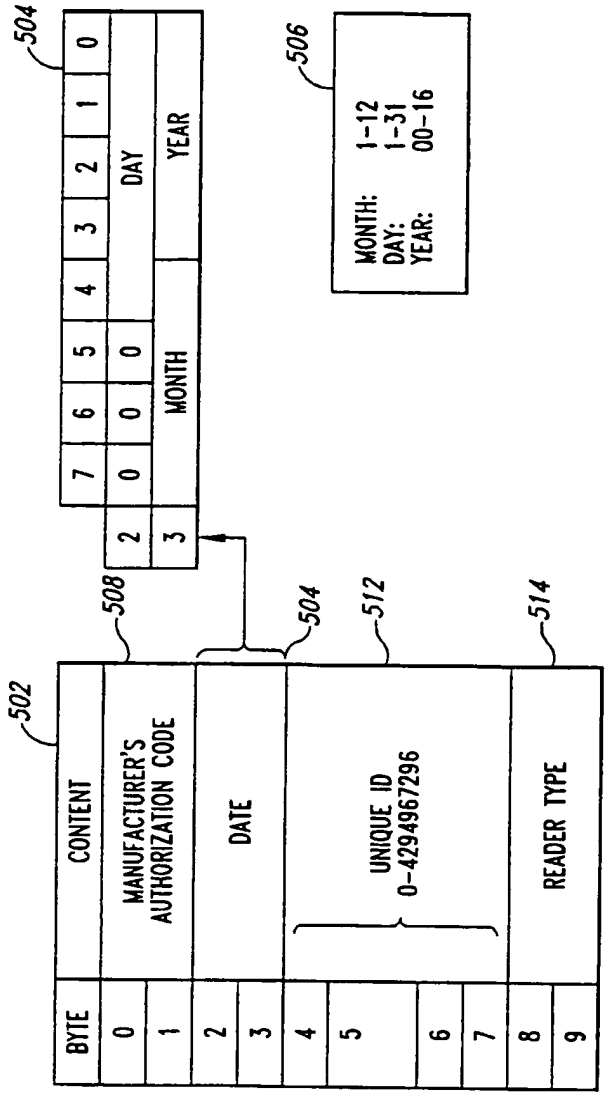

504
7 6 5 4 3 2 1 0
0 0 0 DAY
MONTH YEAR
2 3
506
MONTH: 1-12
DAY: 1-31
YEAR: 00-16
502
508
504
512
514
BYTE
CONTENT
MANUFACTURER'S AUTHORIZATION CODE
DATE
UNIQUE ID 0-4294967296
READER TYPE
0 1 2 3 4 5 6 7 8 9

Fig. 5

BYTE	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
0	M07	M06	M05	M04	M03	M02	M01	M00
1	M15	M14	M13	M12	M11	M10	M09	M08
2	D07	D06	D05	D04	D03	D02	D01	D00
3	D15	D14	D13	D12	D11	D10	D09	D08
4	I07	I06	I05	I04	I03	I02	I01	I00
5	I15	I14	I13	I12	I11	I10	I09	I08
6	I23	I22	I21	I20	I19	I18	I17	I16
7	I31	I30	I29	I28	I27	I26	I25	I24
8	R07	R06	R05	R04	R03	R02	R01	R00
9	R15	R14	R13	R12	R11	R10	R09	R08
10	C07	C06	C05	C04	C03	C02	C01	C00
11	C15	C14	C13	C12	C11	C10	C09	C08
12	C23	C22	C21	C20	C19	C18	C17	C16
13	C31	C30	C29	C28	C27	C26	C25	C24
14	C39	C38	C37	C36	C35	C34	C33	C32
15	C47	C46	C45	C44	C43	C42	C41	C40
16	C55	C54	C53	C52	C51	C50	C49	C48
17	C63	C62	C61	C60	C59	C58	C57	C56
18	V07	V06	V05	V04	V03	V02	V01	V00
19	V15	V14	V13	V12	V11	V10	V09	V08

602

604 READER INFO

606 CHIPPO INFO

608 CHAPP INFO

Fig. 6

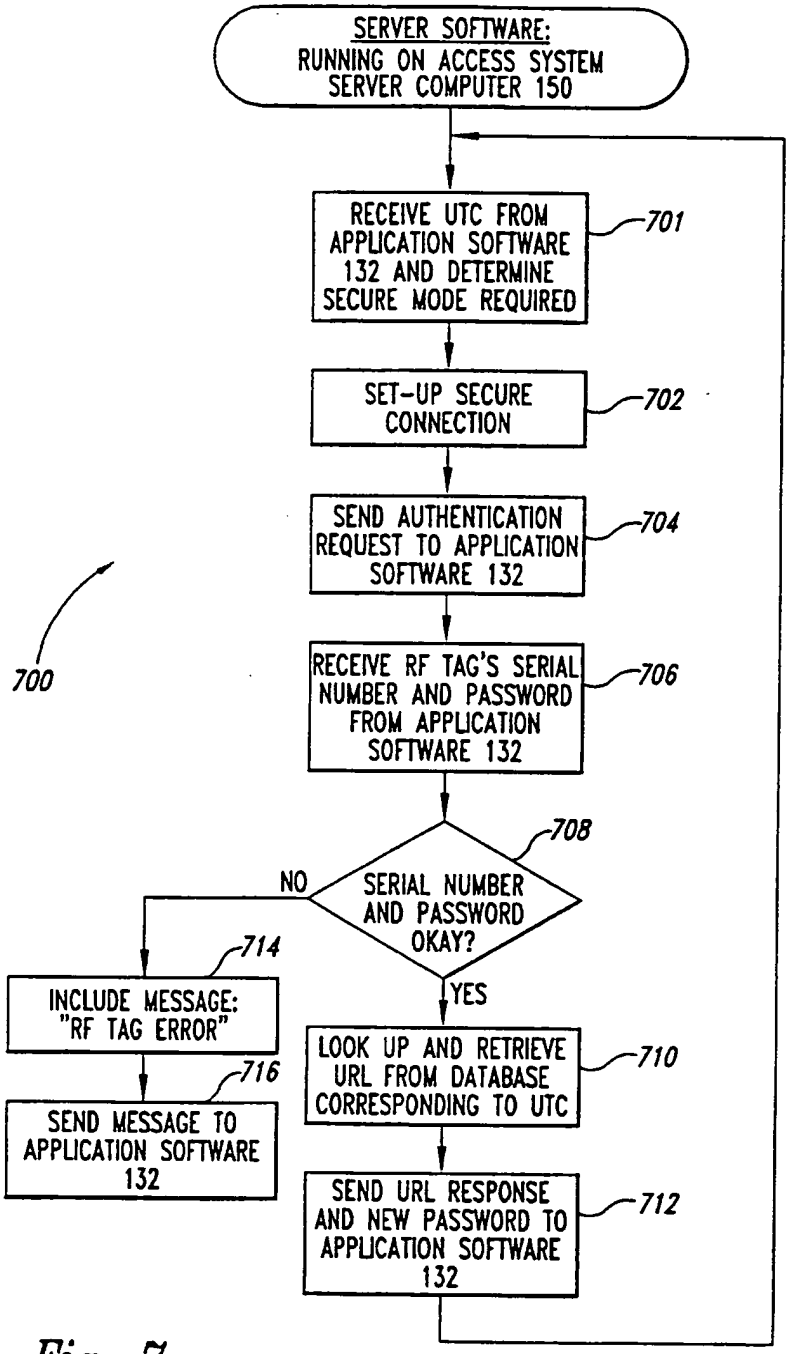

SERVER SOFTWARE:
RUNNING ON ACCESS SYSTEM SERVER COMPUTER 150
RECEIVE UTC FROM APPLICATION SOFTWARE 132 AND DETERMINE SECURE MODE REQUIRED
701
SET-UP SECURE CONNECTION
702
SEND AUTHENTICATION REQUEST TO APPLICATION SOFTWARE 132
704
700
RECEIVE RF TAG'S SERIAL NUMBER AND PASSWORD FROM APPLICATION SOFTWARE 132
706
708
SERIAL NUMBER AND PASSWORD OKAY?
NO
YES
714
INCLUDE MESSAGE: "RF TAG ERROR"
716
SEND MESSAGE TO APPLICATION SOFTWARE 132
LOOK UP AND RETRIEVE URL FROM DATABASE CORRESPONDING TO UTC
710
SEND URL RESPONSE AND NEW PASSWORD TO APPLICATION SOFTWARE 132
712

Fig. 7

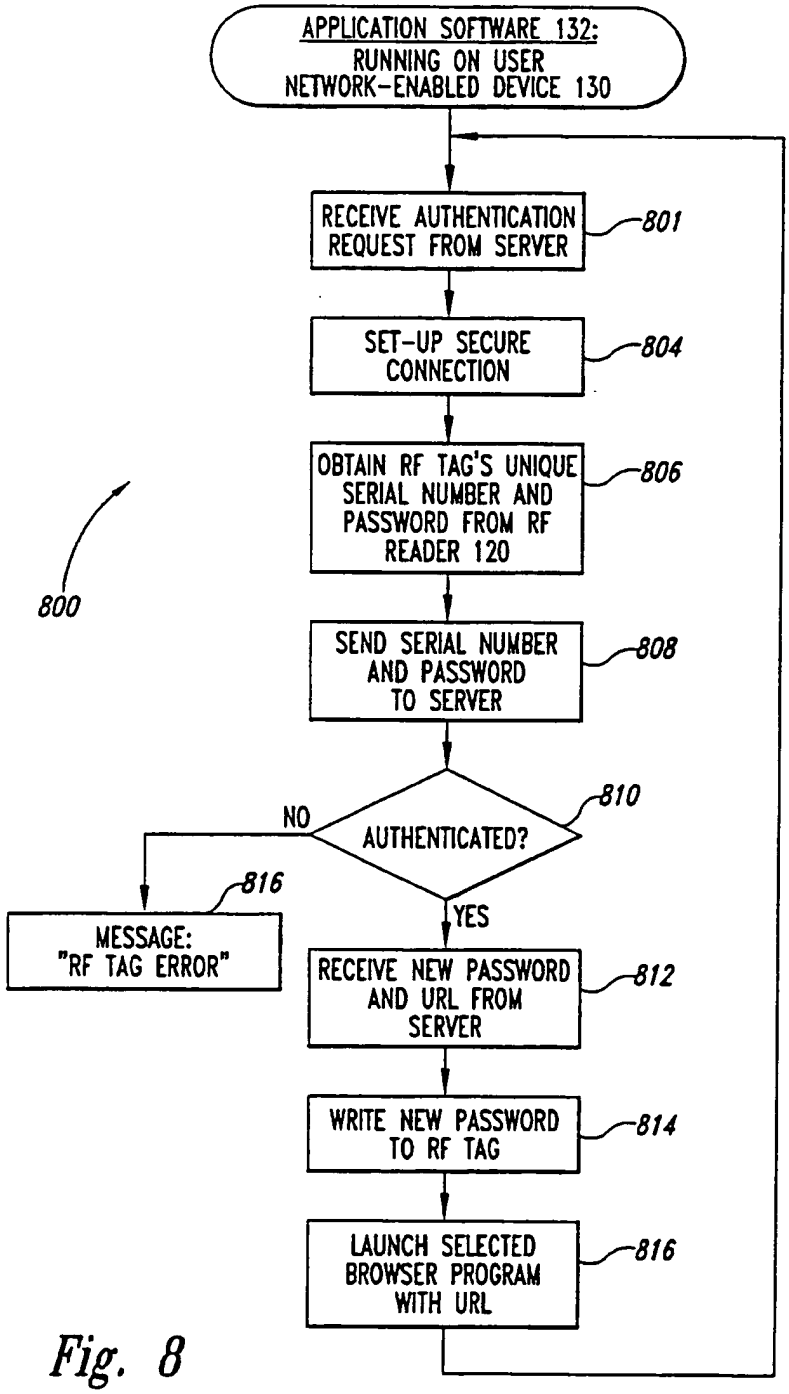

APPLICATION SOFTWARE 132: RUNNING ON USER NETWORK-ENABLED DEVICE 130
RECEIVE AUTHENTICATION REQUEST FROM SERVER
801
SET-UP SECURE CONNECTION
804
OBTAIN RF TAG'S UNIQUE SERIAL NUMBER AND PASSWORD FROM RF READER 120
806
800
SEND SERIAL NUMBER AND PASSWORD TO SERVER
808
AUTHENTICATED?
810
NO
YES
MESSAGE: "RF TAG ERROR"
816
RECEIVE NEW PASSWORD AND URL FROM SERVER
812
WRITE NEW PASSWORD TO RF TAG
814
LAUNCH SELECTED BROWSER PROGRAM WITH URL
816

Fig. 8

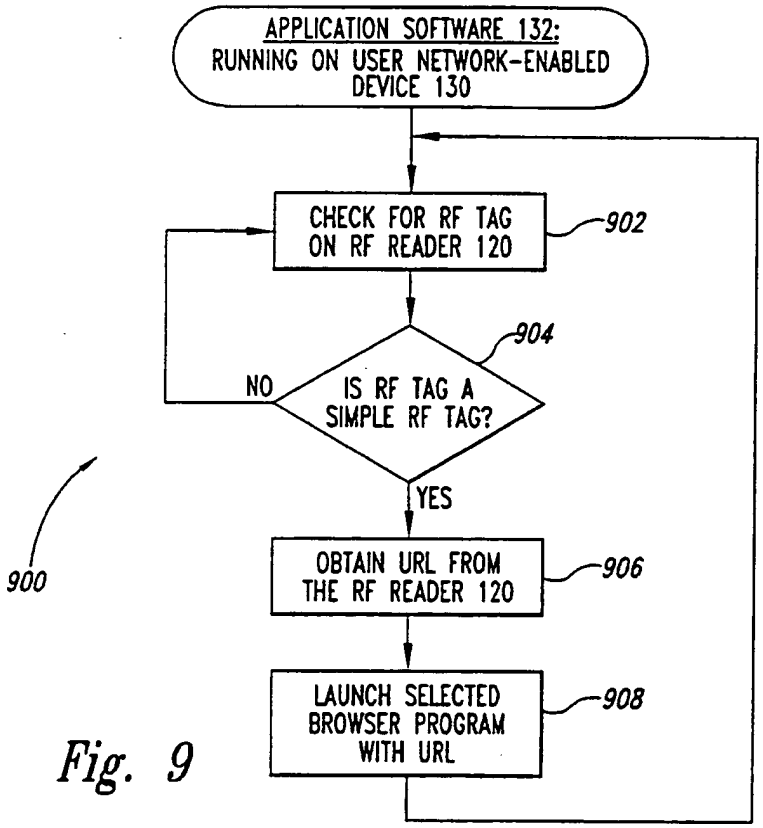

APPLICATION SOFTWARE 132:
RUNNING ON USER NETWORK-ENABLED DEVICE 130
CHECK FOR RF TAG ON RF READER 120
902
904
NO
IS RF TAG A SIMPLE RF TAG?
YES
900
OBTAIN URL FROM THE RF READER 120
906
LAUNCH SELECTED BROWSER PROGRAM WITH URL
908

Fig. 9

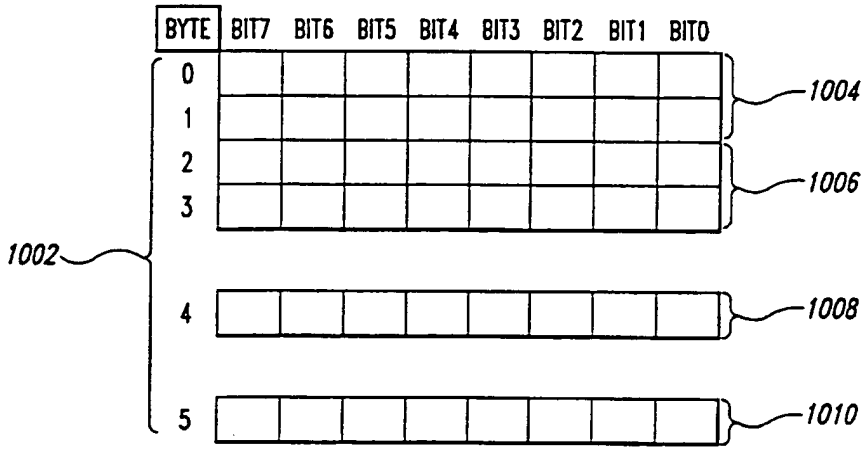

BYTE
BIT7
BIT6
BIT5
BIT4
BIT3
BIT2
BIT1
BIT0
0
1
2
3
4
5
1002
1004
1006
1008
1010

Fig. 10

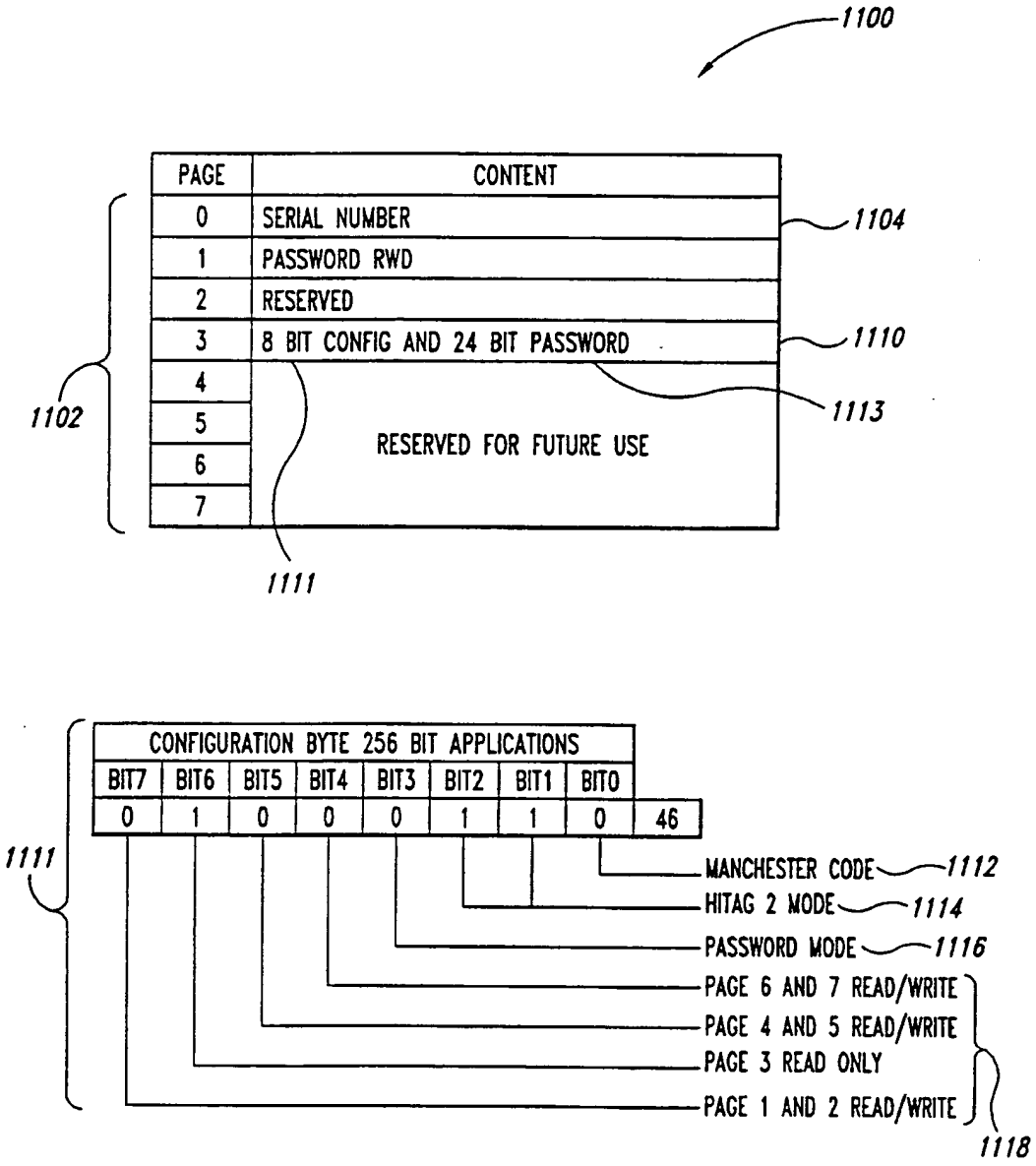

1100
PAGE
CONTENT
0
SERIAL NUMBER
1
PASSWORD RWD
2
RESERVED
3
8 BIT CONFIG AND 24 BIT PASSWORD
4
5
6
7
RESERVED FOR FUTURE USE
1104
1110
1113
1102
1111
CONFIGURATION BYTE 256 BIT APPLICATIONS
BIT7 BIT6 BIT5 BIT4 BIT3 BIT2 BIT1 BIT0
0 1 0 0 0 1 1 0 46
MANCHESTER CODE
HITAG 2 MODE
PASSWORD MODE
PAGE 6 AND 7 READ/WRITE
PAGE 4 AND 5 READ/WRITE
PAGE 3 READ ONLY
PAGE 1 AND 2 READ/WRITE
1112
1114
1116
1118
1111

Fig. 11

1200

BYTE	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0	
0	P07	P06	P05	P04	P03	P02	P01	P00	1202
1	P15	P14	P13	P12	P11	P10	P09	P08	
2	V07	V06	V05	V04	V03	V02	V01	V00	1204
3	V15	V14	V13	V12	V11	V10	V09	V08	
4	M07	M06	M05	M04	M03	M02	M01	M00	1206
5	A07	A06	A05	A04	A03	A02	A01	A00	1208
6	A15	A14	A13	A12	A11	A10	A09	A08	

Fig. 12

1302

BYTE	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0	
0	P07	P06	P05	P04	P03	P02	P01	P00	1304
1	P15	P14	P13	P12	P11	P10	P09	P08	
2	R07	R06	R05	R04	R03	R02	R01	R00	1306
3	R15	R14	R13	R12	R11	R10	R09	R08	
4	R23	R22	R21	R20	R19	R18	R17	R16	
5	R31	R30	R29	R28	R27	R26	R25	R24	
6	C07	C06	C05	C04	C03	C02	C01	C00	1308
7	C15	C14	C13	C12	C11	C10	C09	C08	
8	C23	C22	C21	C20	C19	C18	C17	C16	
9	C31	C30	C29	C28	C27	C26	C25	C24	
10	C39	C38	C37	C36	C35	C34	C33	C32	
11	C47	C46	C45	C44	C43	C42	C41	C40	
12	C55	C54	C53	C52	C51	C50	C49	C48	
13	C63	C62	C61	C60	C59	C58	C57	C56	
14	V07	V06	V05	V04	V03	V02	V01	V00	1310
15	V15	V14	V13	V12	V11	V10	V09	V08	

Fig. 13

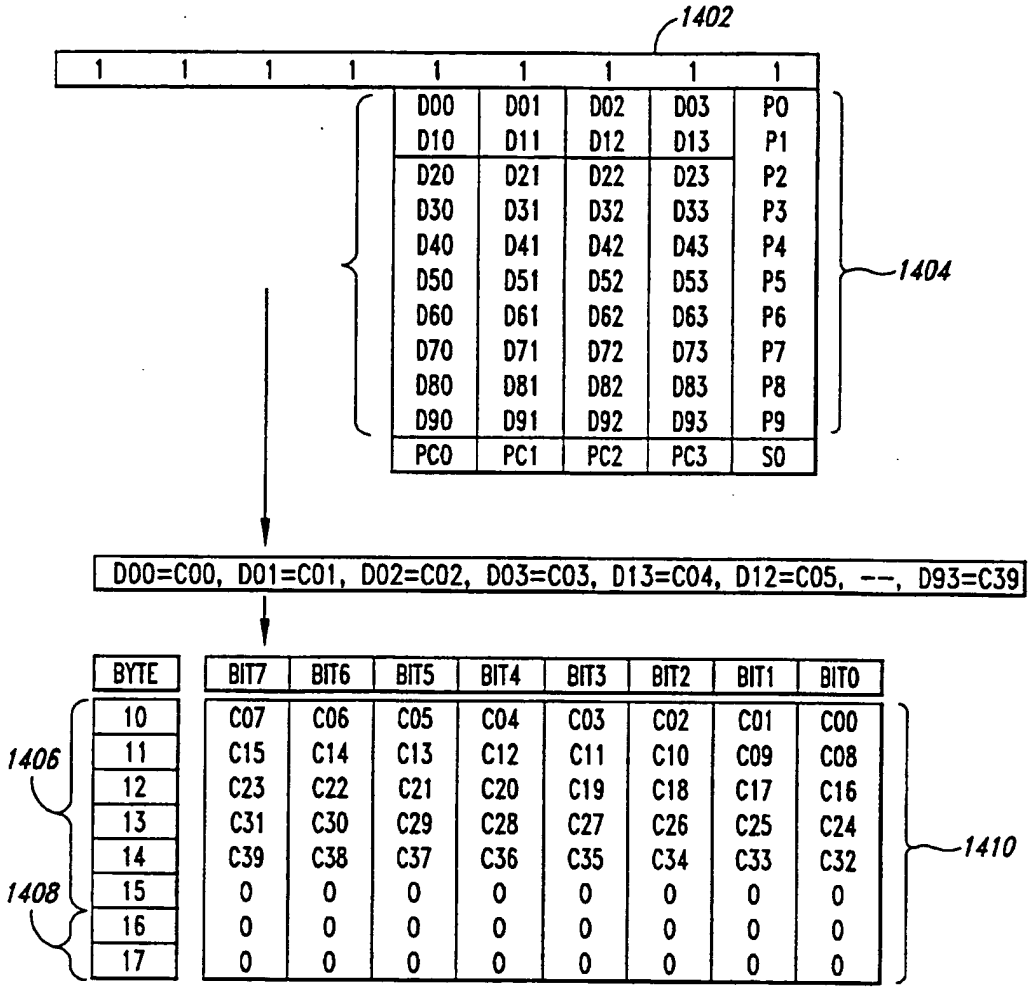

1402
1 1 1 1 1 1 1 1 1
D00 D01 D02 D03 P0
D10 D11 D12 D13 P1
D20 D21 D22 D23 P2
D30 D31 D32 D33 P3
D40 D41 D42 D43 P4
D50 D51 D52 D53 P5
D60 D61 D62 D63 P6
D70 D71 D72 D73 P7
D80 D81 D82 D83 P8
D90 D91 D92 D93 P9
PC0 PC1 PC2 PC3 S0
1404
D00=C00, D01=C01, D02=C02, D03=C03, D13=C04, D12=C05, --, D93=C39
BYTE BIT7 BIT6 BIT5 BIT4 BIT3 BIT2 BIT1 BIT0
10 C07 C06 C05 C04 C03 C02 C01 C00
11 C15 C14 C13 C12 C11 C10 C09 C08
12 C23 C22 C21 C20 C19 C18 C17 C16
13 C31 C30 C29 C28 C27 C26 C25 C24
14 C39 C38 C37 C36 C35 C34 C33 C32
15 0 0 0 0 0 0 0 0
16 0 0 0 0 0 0 0 0
17 0 0 0 0 0 0 0 0
1406
1408
1410

Fig. 14

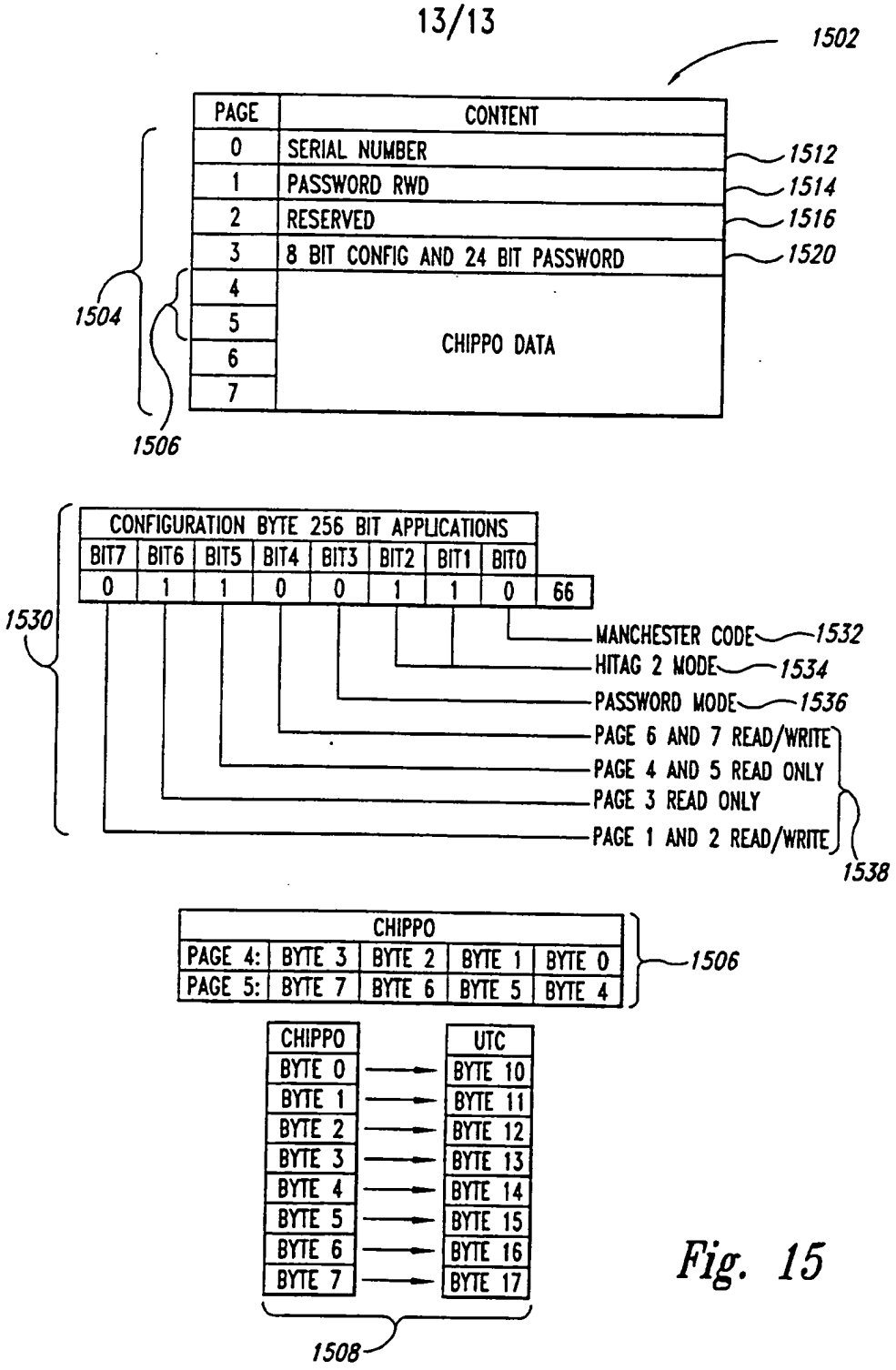

1502
PAGE
CONTENT
0
SERIAL NUMBER
1
PASSWORD RWD
2
RESERVED
3
8 BIT CONFIG AND 24 BIT PASSWORD
4
5
6
7
CHIPPO DATA
1512
1514
1516
1520
1504
1506
CONFIGURATION BYTE 256 BIT APPLICATIONS
BIT7 BIT6 BIT5 BIT4 BIT3 BIT2 BIT1 BIT0
0 1 1 0 0 1 1 0 66
1530
MANCHESTER CODE
HITAG 2 MODE
PASSWORD MODE
PAGE 6 AND 7 READ/WRITE
PAGE 4 AND 5 READ ONLY
PAGE 3 READ ONLY
PAGE 1 AND 2 READ/WRITE
1532
1534
1536
1538
CHIPPO
PAGE 4: BYTE 3 BYTE 2 BYTE 1 BYTE 0
PAGE 5: BYTE 7 BYTE 6 BYTE 5 BYTE 4
1506
CHIPPO
BYTE 0
BYTE 1
BYTE 2
BYTE 3
BYTE 4
BYTE 5
BYTE 6
BYTE 7
UTC
BYTE 10
BYTE 11
BYTE 12
BYTE 13
BYTE 14
BYTE 15
BYTE 16
BYTE 17
1508

Fig. 15